الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

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

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 14th of October to 20th of October. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 14 أكتوبر إلى 20 أكتوبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-21216	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.	2024-10-15	9.8	Critical
CVE-2024-45216	apache software foundation - Apache Solr	Improper Authentication vulnerability in Apache Solr. Solr instances using the PKIAuthenticationPlugin, which is enabled by default when Solr Authentication is used, are vulnerable to Authentication bypass. A fake ending at the end of any Solr API URL path, will allow requests to skip Authentication while maintaining the API contract with the original URL Path. This fake ending looks like an unprotected API path, however it is stripped off internally after authentication but before API routing. This issue affects Apache Solr: from 5.3.0 before 8.11.4, from 9.0.0 before 9.7.0. Users are recommended to upgrade to version 9.7.0, or 8.11.4, which fix the issue.	2024-10-16	9.8	Critical
CVE-2024-43566	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-10-17	9.8	Critical
CVE-2024-9264	grafana - Grafana	The SQL Expressions experimental feature of Grafana allows for the evaluation of `duckdb` queries containing user input. These queries are insufficiently sanitized before being passed to `duckdb`, leading to a command injection and local file inclusion vulnerability. Any user with the VIEWER or higher permission is capable of executing this attack. The `duckdb` binary must be present in Grafana's $PATH for this attack to function; by default, this binary is not installed in Grafana distributions.	2024-10-18	9.4	Critical
CVE-2024-10004	mozilla - Firefox for iOS	Opening an external link to an HTTP website when Firefox iOS was previously closed and had an HTTPS tab open could in some cases result in the padlock icon showing an HTTPS indicator incorrectly This vulnerability affects Firefox for iOS < 131.2.	2024-10-15	9.1	Critical
CVE-2024-37404	ivanti - multiple products	Improper Input Validation in the admin portal of Ivanti Connect Secure before 22.7R2.1 and 9.1R18.9, or Ivanti Policy Secure before 22.7R1.1 allows a remote authenticated attacker to achieve remote code execution.	2024-10-18	9.1	Critical
CVE-2024-21172	oracle - multiple products	Vulnerability in the Oracle Hospitality OPERA 5 product of Oracle Hospitality Applications (component: Opera Servlet). Supported versions that are affected are 5.6.19.19, 5.6.25.8 and 5.6.26.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5. While the vulnerability is in Oracle Hospitality OPERA 5, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hospitality OPERA 5.	2024-10-15	9.0	Critical
CVE-2024-9348	docker - Docker Desktop	Docker Desktop before v4.34.3 allows RCE via unsanitized GitHub source link in Build view.	2024-10-16	8.9	High
CVE-2023-50780	apache - activemq_artemis	Apache ActiveMQ Artemis allows access to diagnostic information and controls through MBeans, which are also exposed through the authenticated Jolokia endpoint. Before version 2.29.0, this also included the Log4J2 MBean. This MBean is not meant for exposure to	2024-10-14	8.8	High

		non-administrative users. This could eventually allow an authenticated attacker to write arbitrary files to the filesystem and indirectly achieve RCE. Users are recommended to upgrade to version 2.29.0 or later, which fixes the issue.			
CVE-2024-21254	oracle - multiple products	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 7.0.0.0.0, 7.6.0.0.0 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 takeover of Oracle BI Publisher.	2024-10-15	8.8	High
CVE-2024-21255	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: XMLPublisher). Supported versions that are affected are 8.59, 8.60 and 8.61. 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 takeover of PeopleSoft Enterprise PeopleTools.	2024-10-15	8.8	High
CVE-2024-9954	google - chrome	Use after free in AI in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-10-15	8.8	High
CVE-2024-9955	google - Chrome	Use after free in WebAuthentication in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2024-10-15	8.8	High
CVE-2024-9957	google - Chrome	Use after free in UI in Google Chrome on iOS prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2024-10-15	8.8	High
CVE-2024-9959	google - Chrome	Use after free in DevTools in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: Medium)	2024-10-15	8.8	High
CVE-2024-9960	google - Chrome	Use after free in Dawn in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2024-10-15	8.8	High
CVE-2024-9961	google - Chrome	Use after free in ParcelTracking in Google Chrome on iOS prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2024-10-15	8.8	High
CVE-2024-9965	google - chrome	Insufficient data validation in DevTools in Google Chrome on Windows prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Low)	2024-10-15	8.8	High
CVE-2024-45693	apache - multiple products	Users logged into the Apache CloudStack's web interface can be tricked to submit malicious CSRF requests due to missing validation of the origin of the requests. This can allow an attacker to gain privileges and access to resources of the authenticated users and may lead to account takeover, disruption, exposure of sensitive data and compromise integrity of the resources owned by the user account that are managed by the platform. This issue affects Apache CloudStack from 4.15.1.0 through 4.18.2.3 and 4.19.0.0 through 4.19.1.1 Users are recommended to upgrade to Apache CloudStack 4.18.2.4 or 4.19.1.2, or later, which addresses this issue.	2024-10-16	8.8	High
CVE-2024-45711	solarwinds - serv-u	SolarWinds Serv-U is vulnerable to a directory traversal vulnerability where remote code execution is possible depending on privileges given to the authenticated user. This issue requires a user to be authenticated and this is present when software environment variables are abused. Authentication is required for this vulnerability	2024-10-16	8.8	High
CVE-2024-20420	cisco - ata_191_firmware	A vulnerability in the web-based management interface of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an authenticated, remote attacker with low privileges to run commands as an Admin user. This vulnerability is due to incorrect authorization verification by the HTTP server. An attacker could exploit this vulnerability by sending a malicious request to the web-based management interface. A successful exploit could allow the attacker to run commands as the Admin user.	2024-10-16	8.8	High
CVE-2024-38814	vmware - multiple products	An authenticated SQL injection vulnerability in VMware HCX was privately reported to VMware. A malicious authenticated user with non-administrator privileges may be able to enter specially crafted SQL queries and perform unauthorized remote code execution on the HCX manager.	2024-10-16	8.8	High
CVE-2024-43595	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-10-17	8.8	High
CVE-2024-43596	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-10-17	8.8	High
CVE-2024-38139	microsoft - Microsoft Dataverse	Improper authentication in Microsoft Dataverse allows an authorized attacker to elevate privileges over a network.	2024-10-15	8.7	High

CVE-2024-38190	microsoft - Microsoft Power Platform	Missing authorization in Power Platform allows an unauthenticated attacker to view sensitive information through a network attack vector.	2024-10-15	8.6	High
CVE-2024-45844	f5 - BIG-IP	BIG-IP monitor functionality may allow an attacker to bypass access control restrictions, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-10-16	8.6	High
CVE-2024-45219	apache software foundation - Apache CloudStack	Account users in Apache CloudStack by default are allowed to upload and register templates for deploying instances and volumes for attaching them as data disks to their existing instances. Due to missing validation checks for KVM-compatible templates or volumes in CloudStack 4.0.0 through 4.18.2.3 and 4.19.0.0 through 4.19.1.1, an attacker that can upload or register templates and volumes, can use them to deploy malicious instances or attach uploaded volumes to their existing instances on KVM-based environments and exploit this to gain access to the host filesystems that could result in the compromise of resource integrity and confidentiality, data loss, denial of service, and availability of KVM-based infrastructure managed by CloudStack. Users are recommended to upgrade to Apache CloudStack 4.18.2.4 or 4.19.1.2, or later, which addresses this issue. Additionally, all user-uploaded or registered KVM-compatible templates and volumes can be scanned and checked that they are flat files that should not be using any additional or unnecessary features. For example, operators can run this on their secondary storage(s) and inspect output. An empty output for the disk being validated means it has no references to the host filesystems; on the other hand, if the output for the disk being validated is not empty, it might indicate a compromised disk. for file in $(find /path/to/storage/ -type f -regex [a-f0-9\-]*.*); do echo "Retrieving file [$file] info. If the output is not empty, that might indicate a compromised disk; check it carefully."; qemu-img info -U $file | grep file: ; printf "\n\n"; done The command can also be run for the file-based primary storages; however, bear in mind that (i) volumes created from templates will have references for the templates at first and (ii) volumes can be consolidated while migrating, losing their references to the templates. Therefore, the command execution for the primary storages can show both false positives and false negatives.For checking the whole template/volume features of each disk, operators can run the following command: for file in $(find /path/to/storage/ -type f -regex [a-f0-9\-]*.*); do echo "Retrieving file [$file] info."; qemu-img info -U $file; printf "\n\n"; done	2024-10-16	8.5	High
CVE-2024-43578	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-10-17	8.3	High
CVE-2024-43579	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-10-17	8.3	High
CVE-2024-20458	cisco - ata_191_firmware	A vulnerability in the web-based management interface of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to view or delete the configuration or change the firmware on an affected device. This vulnerability is due to a lack of authentication on specific HTTP endpoints. An attacker could exploit this vulnerability by browsing to a specific URL. A successful exploit could allow the attacker to view or delete the configuration or change the firmware.	2024-10-16	8.2	High
CVE-2024-21214	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Query). Supported versions that are affected are 8.59, 8.60 and 8.61. 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 creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data.	2024-10-15	8.1	High
CVE-2024-21252	oracle - product_hub	Vulnerability in the Oracle Product Hub product of Oracle E-Business Suite (component: Item Catalog). 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 Product Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Product Hub accessible data as well as unauthorized access to critical data or complete access to all Oracle Product Hub accessible data.	2024-10-15	8.1	High
CVE-2024-21265	oracle - e-business_suite	Vulnerability in the Oracle Site Hub product of Oracle E-Business Suite (component: Site Hierarchy Flows). 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 Site Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Site Hub accessible data as well as unauthorized access to critical data or complete access to all Oracle Site Hub accessible data.	2024-10-15	8.1	High

CVE-2024-21266	oracle - e-business_suite	Vulnerability in the Oracle Advanced Pricing product of Oracle E-Business Suite (component: Price List). 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 Advanced Pricing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Pricing accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Pricing accessible data.	2024-10-15	8.1	High
CVE-2024-21267	oracle - e-business_suite	Vulnerability in the Oracle Cost Management product of Oracle E-Business Suite (component: Cost Planning). Supported versions that are affected are 12.2.12-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Cost Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Cost Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Cost Management accessible data.	2024-10-15	8.1	High
CVE-2024-21268	oracle - e-business_suite	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.2.11-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data.	2024-10-15	8.1	High
CVE-2024-21269	oracle - e-business_suite	Vulnerability in the Oracle Incentive Compensation product of Oracle E-Business Suite (component: Compensation Plan). 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 Incentive Compensation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Incentive Compensation accessible data as well as unauthorized access to critical data or complete access to all Oracle Incentive Compensation accessible data.	2024-10-15	8.1	High
CVE-2024-21270	oracle - e-business_suite	Vulnerability in the Oracle Common Applications Calendar product of Oracle E-Business Suite (component: Tasks). Supported versions that are affected are 12.2.6-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Common Applications Calendar. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Common Applications Calendar accessible data as well as unauthorized access to critical data or complete access to all Oracle Common Applications Calendar accessible data.	2024-10-15	8.1	High
CVE-2024-21271	oracle - e-business_suite	Vulnerability in the Oracle Field Service product of Oracle E-Business Suite (component: Field Service Engineer Portal). 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 Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Field Service accessible data as well as unauthorized access to critical data or complete access to all Oracle Field Service accessible data.	2024-10-15	8.1	High
CVE-2024-21275	oracle - e-business_suite	Vulnerability in the Oracle Quoting product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.2.7-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Quoting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Quoting accessible data as well as unauthorized access to critical data or complete access to all Oracle Quoting accessible data.	2024-10-15	8.1	High
CVE-2024-21276	oracle - e-business_suite	Vulnerability in the Oracle Work in Process product of Oracle E-Business Suite (component: Messages). 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 Work in Process. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Work in Process accessible data as well as unauthorized access to critical data or complete access to all Oracle Work in Process accessible data.	2024-10-15	8.1	High
CVE-2024-21277	oracle - e-business_suite	Vulnerability in the Oracle MES for Process Manufacturing product of Oracle E-Business Suite (component: Device Integration). 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 MES for Process Manufacturing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle MES for Process Manufacturing accessible data as well as unauthorized access to critical	2024-10-15	8.1	High

		data or complete access to all Oracle MES for Process Manufacturing accessible data.			
CVE-2024-21278	oracle - e-business_suite	Vulnerability in the Oracle Contract Lifecycle Management for Public Sector product of Oracle E-Business Suite (component: Award Processes). 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 Contract Lifecycle Management for Public Sector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Contract Lifecycle Management for Public Sector accessible data as well as unauthorized access to critical data or complete access to all Oracle Contract Lifecycle Management for Public Sector accessible data.	2024-10-15	8.1	High
CVE-2024-21279	oracle - e-business_suite	Vulnerability in the Oracle Sourcing product of Oracle E-Business Suite (component: Auctions). 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 Sourcing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sourcing accessible data as well as unauthorized access to critical data or complete access to all Oracle Sourcing accessible data.	2024-10-15	8.1	High
CVE-2024-21280	oracle - service_contracts	Vulnerability in the Oracle Service Contracts product of Oracle E-Business Suite (component: Authoring). Supported versions that are affected are 12.2.5-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Service Contracts accessible data as well as unauthorized access to critical data or complete access to all Oracle Service Contracts accessible data.	2024-10-15	8.1	High
CVE-2024-21282	oracle - e-business_suite	Vulnerability in the Oracle Financials product of Oracle E-Business Suite (component: Common Components). 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 Financials. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financials accessible data as well as unauthorized access to critical data or complete access to all Oracle Financials accessible data.	2024-10-15	8.1	High
CVE-2024-21283	oracle - peoplesoft_enterprise	Vulnerability in the PeopleSoft Enterprise HCM Global Payroll Core product of Oracle PeopleSoft (component: Global Payroll for Core). Supported versions that are affected are 9.2.48-9.2.50. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Global Payroll Core. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise HCM Global Payroll Core accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Global Payroll Core accessible data.	2024-10-15	8.1	High
CVE-2024-45217	apache software foundation - Apache Solr	Insecure Default Initialization of Resource vulnerability in Apache Solr. New ConfigSets that are created via a Restore command, which copy a configSet from the backup and give it a new name, are created without setting the "trusted" metadata. ConfigSets that do not contain the flag are trusted implicitly if the metadata is missing, therefore this leads to "trusted" ConfigSets that may not have been created with an Authenticated request. "trusted" ConfigSets are able to load custom code into classloaders, therefore the flag is supposed to only be set when the request that uploads the ConfigSet is Authenticated & Authorized. This issue affects Apache Solr: from 6.6.0 before 8.11.4, from 9.0.0 before 9.7.0. This issue does not affect Solr instances that are secured via Authentication/Authorization. Users are primarily recommended to use Authentication and Authorization when running Solr. However, upgrading to version 9.7.0, or 8.11.4 will mitigate this issue otherwise.	2024-10-16	8.1	High
CVE-2024-43587	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-10-17	8.1	High
CVE-2024-45766	dell - Dell OpenManage Enterprise	Dell OpenManage Enterprise, version(s) OME 4.1 and prior, contain(s) an Improper Control of Generation of Code ('Code Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Code execution.	2024-10-17	8.0	High
CVE-2024-9956	google - Chrome	Inappropriate implementation in WebAuthentication in Google Chrome on Android prior to 130.0.6723.58 allowed a local attacker to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	2024-10-15	7.8	High
CVE-2024-45710	solarwinds - solarwinds_platform	SolarWinds Platform is susceptible to an Uncontrolled Search Path Element Local Privilege Escalation vulnerability. This requires a low privilege account and local access to the affected node machine.	2024-10-16	7.8	High
CVE-2024-29213	ivanti - DSM	Ivanti DSM < version 2024.2 allows authenticated users on the local machine to run code with elevated privileges due to insecure ACL via unspecified attack vector.	2024-10-18	7.8	High

CVE-2024-29821	ivanti - DSM	Ivanti DSM < version 2024.2 allows authenticated users on the local machine to run code with elevated privileges due to insecure ACL via unspecified attack vector.	2024-10-18	7.8	High
CVE-2024-21191	oracle - fusion_middleware	Vulnerability in the Oracle Enterprise Manager Fusion Middleware Control product of Oracle Fusion Middleware (component: FMW Control Plugin). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Manager Fusion Middleware Control. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Manager Fusion Middleware Control, 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 Enterprise Manager Fusion Middleware Control accessible data as well as unauthorized update, insert or delete access to some of Oracle Enterprise Manager Fusion Middleware Control accessible data.	2024-10-15	7.6	High
CVE-2024-21195	oracle - multiple products	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Layout Templates). Supported versions that are affected are 7.0.0.0.0, 7.6.0.0.0 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 access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher.	2024-10-15	7.6	High
CVE-2024-21190	oracle - fusion_middleware	Vulnerability in the Oracle Global Lifecycle Management FMW Installer product of Oracle Fusion Middleware (component: Cloning). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via SFTP to compromise Oracle Global Lifecycle Management FMW Installer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Global Lifecycle Management FMW Installer accessible data.	2024-10-15	7.5	High
CVE-2024-21215	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via 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.	2024-10-15	7.5	High
CVE-2024-21234	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data.	2024-10-15	7.5	High
CVE-2024-21246	oracle - service_bus	Vulnerability in the Oracle Service Bus product of Oracle Fusion Middleware (component: OSB Core Functionality). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Bus. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Service Bus accessible data.	2024-10-15	7.5	High
CVE-2024-21259	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22 and prior to 7.1.2. 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.	2024-10-15	7.5	High
CVE-2024-21260	oracle - multiple products	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server.	2024-10-15	7.5	High
CVE-2024-21272	oracle - mysql	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/Python). Supported versions that are affected are 9.0.0 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in takeover of MySQL Connectors.	2024-10-15	7.5	High

CVE-2024-21274	oracle - weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via 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.	2024-10-15	7.5	High
CVE-2024-38204	microsoft - Microsoft Azure Functions	Improper Access Control in Imagine Cup allows an authorized attacker to elevate privileges over a network.	2024-10-15	7.5	High
CVE-2024-20459	cisco - ata_191_firmware	A vulnerability in the web-based management interface of Cisco ATA 190 Multiplatform Series Analog Telephone Adapter firmware could allow an authenticated, remote attacker with high privileges to execute arbitrary commands as the root user on the underlying operating system. This vulnerability is due to a lack of input sanitization in the web-based management interface. An attacker could exploit this vulnerability by sending a malicious request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system as the root user.	2024-10-16	7.2	High
CVE-2024-47487	hikvision - hikcentral_professional	There is a SQL injection vulnerability in some HikCentral Professional versions. This could allow an authenticated user to execute arbitrary SQL queries.	2024-10-18	7.2	High
CVE-2024-21284	oracle - banking_liquidity_management	Vulnerability in the Oracle Banking Liquidity Management product of Oracle Financial Services Applications (component: Reports). The supported version that is affected is 14.5.0.12.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Liquidity Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Banking Liquidity Management.	2024-10-15	7.1	High
CVE-2024-21285	oracle - banking_liquidity_management	Vulnerability in the Oracle Banking Liquidity Management product of Oracle Financial Services Applications (component: Reports). The supported version that is affected is 14.5.0.12.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Liquidity Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Banking Liquidity Management.	2024-10-15	7.1	High
CVE-2024-45462	apache - multiple products	The logout operation in the CloudStack web interface does not expire the user session completely which is valid until expiry by time or restart of the backend service. An attacker that has access to a user's browser can use an unexpired session to gain access to resources owned by the logged out user account. This issue affects Apache CloudStack from 4.15.1.0 through 4.18.2.3; and from 4.19.0.0 through 4.19.1.1. Users are recommended to upgrade to Apache CloudStack 4.18.2.4 or 4.19.1.2, or later, which addresses this issue.	2024-10-16	7.1	High
CVE-2024-45715	solarwinds - SolarWinds Platform	The SolarWinds Platform was susceptible to a Cross-Site Scripting vulnerability when performing an edit function to existing elements.	2024-10-16	7.1	High
CVE-2024-20463	cisco - ata_191_firmware	A vulnerability in the web-based management interface of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to modify the configuration or reboot an affected device. This vulnerability is due to the HTTP server allowing state changes in GET requests. An attacker could exploit this vulnerability by sending a malicious request to the web-based management interface on an affected device. A successful exploit could allow the attacker to make limited modifications to the configuration or reboot the device, resulting in a denial of service (DoS) condition.	2024-10-16	7.1	High
CVE-2024-35518	netgear - ex6120_firmware	Netgear EX6120 v1.0.0.68 is vulnerable to Command Injection in genie_fix2.cgi via the wan_dns1_pri parameter.	2024-10-14	6.8	Medium
CVE-2024-35519	netgear - ex3700_firmware	Netgear EX6120 v1.0.0.68, Netgear EX6100 v1.0.2.28, and Netgear EX3700 v1.0.0.96 are vulnerable to command injection in operating_mode.cgi via the ap_mode parameter.	2024-10-14	6.8	Medium
CVE-2024-35520	netgear - r7000_firmware	Netgear R7000 1.0.11.136 is vulnerable to Command Injection in RMT_invite.cgi via device_name2 parameter.	2024-10-14	6.8	Medium
CVE-2024-9676	red hat - multiple products	A vulnerability was found in Podman, Buildah, and CRI-O. A symlink traversal vulnerability in the containers/storage library can cause Podman, Buildah, and CRI-O to hang and result in a denial of service via OOM kill when running a malicious image using an automatically assigned user namespace (`--userns=auto` in Podman and Buildah). The containers/storage library will read /etc/passwd inside the container, but does not properly validate if that file is a symlink, which can be used to cause the library to read an arbitrary file on the host.	2024-10-15	6.5	Medium
CVE-2024-21196	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: X Plugin). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of	2024-10-15	6.5	Medium

		this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.			
CVE-2024-21205	oracle - fusion_middleware	Vulnerability in the Oracle Service Bus product of Oracle Fusion Middleware (component: OSB Core Functionality). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Service Bus. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Service Bus accessible data.	2024-10-15	6.5	Medium
CVE-2024-21230	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	6.5	Medium
CVE-2024-21262	oracle - mysql	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/ODBC). Supported versions that are affected are 9.0.0 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors.	2024-10-15	6.5	Medium
CVE-2024-20421	cisco - ata_191_firmware	A vulnerability in the web-based management interface of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the affected device with the privileges of the targeted user.	2024-10-16	6.5	Medium
CVE-2024-45461	apache - multiple products	The CloudStack Quota feature allows cloud administrators to implement a quota or usage limit system for cloud resources, and is disabled by default. In environments where the feature is enabled, due to missing access check enforcements, non-administrative CloudStack user accounts are able to access and modify quota-related configurations and data. This issue affects Apache CloudStack from 4.7.0 through 4.18.2.3; and from 4.19.0.0 through 4.19.1.1, where the Quota feature is enabled. Users are recommended to upgrade to Apache CloudStack 4.18.2.4 or 4.19.1.2, or later, which addresses this issue. Alternatively, users that do not use the Quota feature are advised to disabled the plugin by setting the global setting "quota.enable.service" to "false".	2024-10-16	6.3	Medium
CVE-2024-20280	cisco - Cisco Unified Computing System Central Software	A vulnerability in the backup feature of Cisco UCS Central Software could allow an attacker with access to a backup file to learn sensitive information that is stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method that is used for the backup function. An attacker could exploit this vulnerability by accessing a backup file and leveraging a static key that is used for the backup configuration feature. A successful exploit could allow an attacker with access to a backup file to learn sensitive information that is stored in full state backup files and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and the device SSL server certificate and key.	2024-10-16	6.3	Medium
CVE-2024-47240	dell - secure_connect_gateway	Dell Secure Connect Gateway (SCG) 5.24 contains an Incorrect Default Permissions vulnerability. A local attacker with low privileges can access the file system and could potentially exploit this vulnerability to gain write access to unauthorized data and cause a version update failure condition.	2024-10-18	6.3	Medium
CVE-2024-21202	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.59, 8.60 and 8.61. 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.	2024-10-15	6.1	Medium
CVE-2024-21263	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22 and prior to 7.1.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability	2024-10-15	6.1	Medium

		to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox and unauthorized read access to a subset of Oracle VM VirtualBox accessible data.			
CVE-2024-20460	cisco - ata_191_firmware	A vulnerability in the web-based management interface of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user&nbsp;to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information on an affected device.	2024-10-16	6.1	Medium
CVE-2024-20512	cisco - Cisco Unified Contact Center Management Portal	A vulnerability in the web-based management interface of Cisco Unified Contact Center Management Portal (Unified CCMP) could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	2024-10-16	6.1	Medium
CVE-2024-21273	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22 and prior to 7.1.2. 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.	2024-10-15	6.0	Medium
CVE-2024-20461	cisco - ata_191_firmware	A vulnerability in the CLI of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an authenticated, local attacker with high privileges to execute arbitrary commands as the root user. This vulnerability exists because CLI input is not properly sanitized. An attacker could exploit this vulnerability by sending malicious characters to the CLI. A successful exploit could allow the attacker to read and write to the underlying operating system as the root user.	2024-10-16	6.0	Medium
CVE-2024-45085	ibm - WebSphere Application Server	IBM WebSphere Application Server 8.5 is vulnerable to a denial of service, under certain configurations, caused by an unexpected specially crafted request. A remote attacker could exploit this vulnerability to cause an error resulting in a denial of service.	2024-10-15	5.9	Medium
CVE-2024-4184	microfocus - application_automation_tools	Improper Restriction of XML External Entity Reference vulnerability in OpenText Application Automation Tools allows DTD Injection. This issue affects OpenText Application Automation Tools: 24.1.0 and below.	2024-10-16	5.9	Medium
CVE-2024-4189	microfocus - application_automation_tools	Improper Restriction of XML External Entity Reference vulnerability in OpenText Application Automation Tools allows DTD Injection. This issue affects OpenText Application Automation Tools: 24.1.0 and below.	2024-10-16	5.9	Medium
CVE-2024-47674	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mm: avoid leaving partial pfn mappings around in error case As Jann points out, PFN mappings are special, because unlike normal memory mappings, there is no lifetime information associated with the mapping - it is just a raw mapping of PFNs with no reference counting of a 'struct page'. That's all very much intentional, but it does mean that it's easy to mess up the cleanup in case of errors. Yes, a failed mmap() will always eventually clean up any partial mappings, but without any explicit lifetime in the page table mapping itself, it's very easy to do the error handling in the wrong order. In particular, it's easy to mistakenly free the physical backing store before the page tables are actually cleaned up and (temporarily) have stale dangling PTE entries. To make this situation less error-prone, just make sure that any partial pfn mapping is torn down early, before any other error handling.	2024-10-15	5.5	Medium
CVE-2024-20462	cisco - ata_191_firmware	A vulnerability in the web-based management interface of Cisco ATA 190 Series Multiplatform Analog Telephone Adapter firmware could allow an authenticated, local attacker with low privileges to view passwords on an affected device. This vulnerability is due to incorrect sanitization of HTML content from an affected device. A successful exploit could allow the attacker to view passwords that belong to other users.	2024-10-16	5.5	Medium
CVE-2024-45072	ibm - multiple products	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A privileged user could exploit this vulnerability to expose sensitive information or consume memory resources.	2024-10-16	5.5	Medium
CVE-2024-47459	adobe - substance_3d_sampler	Substance3D - Sampler versions 4.5 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS) condition. An attacker could exploit this vulnerability to crash the application, resulting in a DoS. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-17	5.5	Medium

CVE-2024-47485	hikvision - hikcentral_master	There is a CSV injection vulnerability in some HikCentral Master Lite versions. If exploited, an attacker could build malicious data to generate executable commands in the CSV file.	2024-10-18	5.5	Medium
CVE-2024-47241	dell - Secure Connect Gateway (SCG) 5.0 Appliance - SRS	Dell Secure Connect Gateway (SCG) 5.0 Appliance - SRS, version(s) 5.24, contains an Improper Certificate Validation vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access and modification of transmitted data.	2024-10-18	5.5	Medium
CVE-2024-21286	oracle - peoplesoft_enterprise	Vulnerability in the PeopleSoft Enterprise ELM Enterprise Learning Management product of Oracle PeopleSoft (component: Enterprise Learning Management). 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 ELM Enterprise Learning Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise ELM Enterprise Learning 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 PeopleSoft Enterprise ELM Enterprise Learning Management accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise ELM Enterprise Learning Management accessible data.	2024-10-15	5.4	Medium
CVE-2024-10033	red hat - Red Hat Ansible Automation Platform 2	A vulnerability was found in aap-gateway. A Cross-site Scripting (XSS) vulnerability exists in the gateway component. This flaw allows a malicious user to perform actions that impact users by using the "?next=" in a URL, which can lead to redirecting, injecting malicious script, stealing sessions and data.	2024-10-16	5.4	Medium
CVE-2024-43580	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-10-17	5.4	Medium
CVE-2024-9979	red hat - multiple products	A flaw was found in PyO3. This vulnerability causes a use-after-free issue, potentially leading to memory corruption or crashes via unsound borrowing from weak Python references.	2024-10-15	5.3	Medium
CVE-2024-21238	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.39 and prior, 8.4.1 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	5.3	Medium
CVE-2024-21248	oracle - multiple products	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22 and prior to 7.1.2. Difficult to exploit vulnerability allows low 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 update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as 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.	2024-10-15	5.3	Medium
CVE-2024-21281	oracle - banking_liquidity_management	Vulnerability in the Oracle Banking Liquidity Management product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.7.0.6.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Liquidity Management. 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 Banking Liquidity Management accessible data as well as unauthorized read access to a subset of Oracle Banking Liquidity Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Liquidity Management.	2024-10-15	5.3	Medium
CVE-2024-9966	google - chrome	Inappropriate implementation in Navigations in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	2024-10-15	5.3	Medium
CVE-2024-49023	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-10-18	5.3	Medium
CVE-2024-38820	vmware - multiple products	The fix for CVE-2022-22968 made disallowedFields patterns in DataBinder case insensitive. However, String.toLowerCase() has some Locale dependent exceptions that could potentially result in fields not protected as expected.	2024-10-18	5.3	Medium
CVE-2024-4690	microfocus - application_automation_tools	Improper Restriction of XML External Entity Reference vulnerability in OpenText Application Automation Tools allows DTD Injection.This issue affects OpenText Application Automation Tools: 24.1.0 and below.	2024-10-16	5.1	Medium
CVE-2024-45713	solarwinds - Kiwi CatTools	SolarWinds Kiwi CatTools is susceptible to a sensitive data disclosure vulnerability when a non-default setting has been enabled for troubleshooting purposes.	2024-10-17	5.1	Medium

CVE-2024-21193	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21194	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21197	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21198	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21199	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21200	oracle - mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21201	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21203	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21204	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.4.0 and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21207	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.38 and prior, 8.4.1 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21218	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21219	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are	2024-10-15	4.9	Medium

		8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.			
CVE-2024-21236	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21239	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21241	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.	2024-10-15	4.9	Medium
CVE-2024-21261	oracle - multiple products	Vulnerability in Oracle Application Express (component: General). Supported versions that are affected are 23.2 and 24.1. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Express. While the vulnerability is in Oracle Application Express, 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 Application Express accessible data as well as unauthorized read access to a subset of Oracle Application Express accessible data.	2024-10-15	4.9	Medium
CVE-2024-21235	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. 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.	2024-10-15	4.8	Medium
CVE-2024-45714	solarwinds - Serv-U	Application is vulnerable to Cross Site Scripting (XSS) an authenticated attacker with users' permissions can modify a variable with a payload.	2024-10-16	4.8	Medium
CVE-2024-47139	f5 - BIG-IQ	A stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IQ Configuration utility that allows an attacker with the Administrator role to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-10-16	4.8	Medium
CVE-2024-45071	ibm - multiple products	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-10-16	4.8	Medium
CVE-2024-9683	red hat - Red Hat Quay 3	A vulnerability was found in Quay, which allows successful authentication even when a truncated password version is provided. This flaw affects the authentication mechanism, reducing the overall security of password enforcement. While the risk is relatively low due to the typical length of the passwords used (73 characters), this vulnerability can still be exploited to reduce the complexity of brute-force or password-guessing attacks. The truncation of passwords weakens the overall authentication process, thereby reducing the effectiveness of password policies and potentially increasing the risk of unauthorized access in the future.	2024-10-17	4.8	Medium
CVE-2024-48016	dell - Secure Connect Gateway	Dell Secure Connect Gateway (SCG) 5.0 Appliance - SRS, version(s) 5.24, contains a Use of a Broken or Risky Cryptographic Algorithm	2024-10-18	4.6	Medium

	(SCG) 5.0 Appliance - SRS	vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to information disclosure. The attacker may be able to use exposed credentials to access the system with privileges of the compromised account.			
CVE-2024-21192	oracle - fusion_middleware	Vulnerability in the Oracle Enterprise Manager for Fusion Middleware product of Oracle Fusion Middleware (component: WebLogic Mgmt). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Enterprise Manager for Fusion Middleware executes to compromise Oracle Enterprise Manager for Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Manager for Fusion Middleware accessible data.	2024-10-15	4.4	Medium
CVE-2024-21212	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Health Monitor). Supported versions that are affected are 8.0.39 and prior and 8.4.0. 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.	2024-10-15	4.4	Medium
CVE-2024-21233	oracle - multiple products	Vulnerability in the Oracle Database Core component of Oracle Database Server. Supported versions that are affected are 19.3-19.24, 21.3-21.15 and 23.4-23.5. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database Core. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database Core accessible data.	2024-10-15	4.3	Medium
CVE-2024-9958	google - chrome	Inappropriate implementation in PictureInPicture in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-10-15	4.3	Medium
CVE-2024-9962	google - chrome	Inappropriate implementation in Permissions in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-10-15	4.3	Medium
CVE-2024-9963	google - chrome	Insufficient data validation in Downloads in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-10-15	4.3	Medium
CVE-2024-9964	google - chrome	Inappropriate implementation in Payments in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Low)	2024-10-15	4.3	Medium
CVE-2024-49340	ibm - Watson Studio Local	IBM Watson Studio Local 1.2.3 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.	2024-10-16	4.3	Medium
CVE-2024-45767	dell - Dell OpenManage Enterprise	Dell OpenManage Enterprise, version(s) OME 4.1 and prior, 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 Information disclosure.	2024-10-17	4.3	Medium
CVE-2024-43577	microsoft - Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-10-18	4.3	Medium
CVE-2024-21213	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. 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 MySQL Server.	2024-10-15	4.2	Medium
CVE-2024-21247	oracle - multiple products	Vulnerability in the MySQL Client product of Oracle MySQL (component: Client: mysqldump). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. 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.	2024-10-15	3.8	Low
CVE-2024-21217	oracle - multiple products	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise	2024-10-15	3.7	Low

		Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. 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.			
CVE-2024-21242	oracle - multiple products	Vulnerability in the XML Database component of Oracle Database Server. Supported versions that are affected are 19.3-19.24, 21.3-21.15 and 23.4-23.5. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via HTTP to compromise XML Database. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of XML Database.	2024-10-15	3.5	Low
CVE-2024-21231	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server.	2024-10-15	3.1	Low
CVE-2024-21251	oracle - multiple products	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.24, 21.3-21.15 and 23.4-23.5. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java VM accessible data.	2024-10-15	3.1	Low
CVE-2024-21253	oracle - vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22. 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 ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox.	2024-10-15	2.3	Low
CVE-2024-21232	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server.	2024-10-15	2.2	Low
CVE-2024-21237	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication GCS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server.	2024-10-15	2.2	Low
CVE-2024-21243	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Telemetry). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data.	2024-10-15	2.2	Low
CVE-2024-21244	oracle - multiple products	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Telemetry). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data.	2024-10-15	2.2	Low
CVE-2024-47486	hikvision - hikcentral_master	There is an XSS vulnerability in some HikCentral Master Lite versions. If exploited, an attacker could inject scripts into certain pages by building malicious data.	2024-10-18	2.1	Low
CVE-2024-21209	oracle - multiple products	Vulnerability in the MySQL Client product of Oracle MySQL (component: Client: mysqldump). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. 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 read access to a subset of MySQL Client accessible data.	2024-10-15	2.0	Low

CVE-2024-4211	microfocus - application_automation_tools	Improper Validation of Specified Quantity in Input vulnerability in OpenText OpenText Application Automation Tools allows Exploiting Incorrectly Configured Access Control Security Levels. Multiple missing permission checks - ALM job config has been discovered in OpenText Application Automation Tools. The vulnerability could allow users with Overall/Read permission to enumerate ALM server names, usernames and client IDs configured to be used with ALM servers. This issue affects OpenText Application Automation Tools: 24.1.0 and below.	2024-10-16	1.8	Low
CVE-2024-4692	microfocus - application_automation_tools	Improper Validation of Specified Quantity in Input vulnerability in OpenText OpenText Application Automation Tools allows Exploiting Incorrectly Configured Access Control Security Levels. Multiple missing permission checks - Service Virtualization config has been discovered in in OpenText Application Automation Tools. The vulnerability could allow users with Overall/Read permission to enumerate Service Virtualization server names. This issue affects OpenText Application Automation Tools: 24.1.0 and below.	2024-10-16	1.8	Low

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.