الهيئة الوطنية للأمن السيبراني
Nat onal 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 18th of February to 24th of February. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 18 فبراير إلى 24 فبراير. 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-2024-22245	VMware	Arbitrary Authentication Relay and Session Hijack vulnerabilities in the deprecated VMware Enhanced Authentication Plug-in (EAP) could allow a malicious actor that could trick a target domain user with EAP installed in their web browser into requesting and relaying service tickets for arbitrary Active Directory Service Principal Names (SPNs).	2024-02-20	9.6	Critical
CVE-2024-25147	Liferay	Cross-site scripting (XSS) vulnerability in HtmlUtil.escapeJsLink in Liferay Portal 7.2.0 through 7.4.1, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 15, and older unsupported versions allows remote attackers to inject arbitrary web script or HTML via crafted javascript: style links.	2024-02-21	9.6	Critical
CVE-2023-42496	Liferay	Reflected cross-site scripting (XSS) vulnerability on the add assignees to a role page in Liferay Portal 7.3.3 through 7.4.3.97, and Liferay DXP 2023.Q3 before patch 6, 7.4 GA through update 92, and 7.3 before update 34 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_roles_admin_web_portlet_RolesAdminPortlet_tabs2 parameter.	2024-02-21	9.6	Critical
CVE-2023-42498	Liferay	Reflected cross-site scripting (XSS) vulnerability in the Language Override edit screen in Liferay Portal 7.4.3.8 through 7.4.3.97, and Liferay DXP 2023.Q3 before patch 5, and 7.4 update 4 through 92 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_portal_language_override_web_internal_portlet_PLOPortlet_key parameter.	2024-02-21	9.6	Critical
CVE-2024-26269	Liferay	Cross-site scripting (XSS) vulnerability in the Frontend JS module's portlet.js in Liferay Portal 7.2.0 through 7.4.3.37, and Liferay DXP 7.4 before update 38, 7.3 before update 11, 7.2 before fix pack 20, and older unsupported versions allows remote attackers to inject arbitrary web script or HTML via the anchor (hash) part of a URL.	2024-02-21	9.6	Critical
CVE-2024-25610	Liferay	In Liferay Portal 7.2.0 through 7.4.3.12, and older unsupported versions, and Liferay DXP 7.4 before update 9, 7.3 before update 4, 7.2 before fix pack 19, and older unsupported versions, the default configuration does not sanitize blog entries of JavaScript, which allows remote authenticated users to inject arbitrary web script or HTML (XSS) via a crafted payload injected into a blog entry’s content text field.	2024-02-20	9	Critical
CVE-2024-25152	Liferay	Stored cross-site scripting (XSS) vulnerability in Message Board widget in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML via the filename of an attachment.	2024-02-21	9	Critical
CVE-2024-25601	Liferay	Stored cross-site scripting (XSS) vulnerability in Expando module's geolocation custom fields in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or	2024-02-21	9	Critical

		HTML via a crafted payload injected into the name text field of a geolocation custom field.			
CVE-2024-25602	Liferay	Stored cross-site scripting (XSS) vulnerability in Users Admin module's edit user page in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into an organization's "Name" text field	2024-02-21	9	Critical
CVE-2023-40191	Liferay	Reflected cross-site scripting (XSS) vulnerability in the instance settings for Accounts in Liferay Portal 7.4.3.44 through 7.4.3.97, and Liferay DXP 2023.Q3 before patch 6, and 7.4 update 44 through 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into the "Blocked Email Domains" text field	2024-02-21	9	Critical
CVE-2024-25603	Liferay	Stored cross-site scripting (XSS) vulnerability in the Dynamic Data Mapping module's DDMForm in Liferay Portal 7.2.0 through 7.4.3.4, and older unsupported versions, and Liferay DXP 7.4.13, 7.3 before update 4, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML via the instanceId parameter.	2024-02-21	9	Critical
CVE-2024-26266	Liferay	Multiple stored cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.2.0 through 7.4.3.13, and older unsupported versions, and Liferay DXP 7.4 before update 10, 7.3 before update 4, 7.2 before fix pack 17, and older unsupported versions allow remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into the first/middle/last name text field of the user who creates an entry in the (1) Announcement widget, or (2) Alerts widget.	2024-02-21	9	Critical
CVE-2023-47795	Liferay	Stored cross-site scripting (XSS) vulnerability in the Document and Media widget in Liferay Portal 7.4.3.18 through 7.4.3.101, and Liferay DXP 2023.Q3 before patch 6, and 7.4 update 18 through 92 allows remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into a document's "Title" text field.	2024-02-21	9	Critical
CVE-2023-42791	Fortinet	A relative path traversal in Fortinet FortiManager version 7.4.0 and 7.2.0 through 7.2.3 and 7.0.0 through 7.0.8 and 6.4.0 through 6.4.12 and 6.2.0 through 6.2.11 allows attacker to execute unauthorized code or commands via crafted HTTP requests.	2024-02-20	8.8	High
CVE-2023-29181	Fortinet	A use of externally-controlled format string in Fortinet FortiOS 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14, 6.0.0 through 6.0.16, FortiProxy 7.2.0 through 7.2.4, 7.0.0 through 7.0.10, 2.0.0 through 2.0.12, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiPAM 1.0.0 through 1.0.3 allows attacker to execute unauthorized code or commands via specially crafted command.	2024-02-22	8.8	High
CVE-2022-43842	IBM	IBM Aspera Console 3.4.0 through 3.4.2 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 239079.	2024-02-23	8.6	High
CVE-2024-21678	Atlassian	This High severity Stored XSS vulnerability was introduced in version 2.7.0 of Confluence Data Center. This Stored XSS vulnerability, with a CVSS Score of 8.5, allows an authenticated attacker to execute arbitrary HTML or JavaScript code on a victims browser which has high impact to confidentiality, low impact to integrity, no impact to availability, and requires no user interaction. Data Center Atlassian recommends that Confluence Data Center customers upgrade to the latest version. If you are unable to do so, upgrade your instance to one of the specified supported fixed versions: ||Affected versions||Fixed versions|| |from 8.7.0 to 8.7.1|8.8.0 recommended or 8.7.2| |from 8.6.0 to 8.6.1|8.8.0 recommended| |from 8.5.0 to 8.5.4 LTS|8.8.0 recommended or 8.5.5 LTS or 8.5.6 LTS| |from 8.4.0 to 8.4.5|8.8.0 recommended or 8.5.6 LTS|	2024-02-20	8.5	High

<table>
<tr><th></th><th></th><th></th><th></th><th></th><th></th></tr>
<tr><td></td><td></td><td>|from 8.3.0 to 8.3.4|8.8.0 recommended or 8.5.6 LTS|
from 8.2.0 to 8.2.3	8.8.0 recommended or 8.5.6 LTS
from 8.1.0 to 8.1.4	8.8.0 recommended or 8.5.6 LTS
from 8.0.0 to 8.0.4	8.8.0 recommended or 8.5.6 LTS
from 7.20.0 to 7.20.3	8.8.0 recommended or 8.5.6 LTS
from 7.19.0 to 7.19.17 LTS	8.8.0 recommended or 8.5.6 LTS or 7.19.18 LTS or 7.19.19 LTS
from 7.18.0 to 7.18.3	8.8.0 recommended or 8.5.6 LTS or 7.19.19 LTS
from 7.17.0 to 7.17.5	8.8.0 recommended or 8.5.6 LTS or 7.19.19 LTS
Any earlier versions	8.8.0 recommended or 8.5.6 LTS or 7.19.19 LTS	 Server Atlassian recommends that Confluence Server customers upgrade to the latest 8.5.x LTS version. If you are unable to do so, upgrade your instance to one of the specified supported fixed versions: 		Affected versions		Fixed versions	
from 8.5.0 to 8.5.4 LTS	8.5.5 LTS or 8.5.6 LTS recommended
from 8.4.0 to 8.4.5	8.5.6 LTS recommended
from 8.3.0 to 8.3.4	8.5.6 LTS recommended
from 8.2.0 to 8.2.3	8.5.6 LTS recommended
from 8.1.0 to 8.1.4	8.5.6 LTS recommended
from 8.0.0 to 8.0.4	8.5.6 LTS recommended
from 7.20.0 to 7.20.3	8.5.6 LTS recommended
from 7.19.0 to 7.19.17 LTS	8.5.6 LTS recommended or 7.19.18 LTS or 7.19.19 LTS
from 7.18.0 to 7.18.3	8.5.6 LTS recommended or 7.19.19 LTS
from 7.17.0 to 7.17.5	8.5.6 LTS recommended or 7.19.19 LTS
Any earlier versions	8.5.6 LTS recommended or 7.19.19 LTS	 See the release notes ([https://confluence.atlassian.com/doc/confluence-release-notes-327.html]). You can download the latest version of Confluence Data Center from the download center ([https://www.atlassian.com/software/confluence/download-archives]). This vulnerability was reported via our Bug Bounty program.</td><td></td><td></td><td></td></tr>
<tr><td>CVE-2024-25021</td><td>IBM</td><td>IBM AIX 7.3, VIOS 4.1's Perl implementation could allow a non-privileged local user to exploit a vulnerability to execute arbitrary commands. IBM X-Force ID: 281320.</td><td>2024-02-22</td><td>8.4</td><td>High</td></tr>
<tr><td>CVE-2024-26192</td><td>Microsoft</td><td>Microsoft Edge (Chromium-based) Information Disclosure Vulnerability</td><td>2024-02-23</td><td>8.2</td><td>High</td></tr>
<tr><td>CVE-2023-6764</td><td>Zyxel</td><td></td><td>2024-02-20</td><td>8.1</td><td>High</td></tr>
</table>

متاح

		A format string vulnerability in a function of the IPSec VPN feature in Zyxel ATP series firmware versions from 4.32 through 5.37 Patch 1, USG FLEX series firmware versions from 4.50 through 5.37 Patch 1, USG FLEX 50(W) series firmware versions from 4.16 through 5.37 Patch 1, and USG20(W)-VPN series firmware versions from 4.16 through 5.37 Patch 1 could allow an attacker to achieve unauthorized remote code execution by sending a sequence of specially crafted payloads containing an invalid pointer; however, such an attack would require detailed knowledge of an affected device's memory layout and configuration.			
CVE-2024-25607	Liferay	The default password hashing algorithm (PBKDF2-HMAC-SHA1) in Liferay Portal 7.2.0 through 7.4.3.15, and older unsupported versions, and Liferay DXP 7.4 before update 16, 7.3 before update 4, 7.2 before fix pack 17, and older unsupported versions defaults to a low work factor, which allows attackers to quickly crack password hashes.	2024-02-20	8.1	High
CVE-2024-25606	Liferay	XXE vulnerability in Liferay Portal 7.2.0 through 7.4.3.7, and older unsupported versions, and Liferay DXP 7.4 before update 4, 7.3 before update 12, 7.2 before fix pack 20, and older unsupported versions allows attackers with permission to deploy widgets/portlets/extensions to obtain sensitive information or consume system resources via the Java2WsddTask._format method.	2024-02-20	8	High
CVE-2024-22250	VMware	Session Hijack vulnerability in Deprecated VMware Enhanced Authentication Plug-in could allow a malicious actor with unprivileged local access to a windows operating system can hijack a privileged EAP session when initiated by a privileged domain user on the same system.	2024-02-20	7.8	High
CVE-2023-29180	Fortinet	A null pointer dereference in Fortinet FortiOS version 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14, 6.0.0 through 6.0.16, FortiProxy 7.2.0 through 7.2.3, 7.0.0 through 7.0.10, 2.0.0 through 2.0.12, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to denial of service via specially crafted HTTP requests.	2024-02-22	7.5	High
CVE-2024-1786	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DIR-600M C1 3.08. Affected by this issue is some unknown functionality of the component Telnet Service. The manipulation of the argument username leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254576. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	2024-02-23	7.5	High
CVE-2023-6398	Zyxel	A post-authentication command injection vulnerability in the file upload binary in Zyxel ATP series firmware versions from 4.32 through 5.37 Patch 1, USG FLEX series firmware versions from 4.50 through 5.37 Patch 1, USG FLEX 50(W) series firmware versions from 4.16 through 5.37 Patch 1, USG20(W)-VPN series firmware versions from 4.16 through 5.37 Patch 1, USG FLEX H series firmware versions from 1.10 through 1.10 Patch 1, NWA50AX firmware versions through 6.29(ABYW.3), WAC500 firmware versions through 6.65(ABVS.1), WAX300H firmware versions through 6.60(ACHF.1), and WBE660S firmware versions through 6.65(ACGG.1) could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device via FTP.	2024-02-20	7.2	High
CVE-2024-21682	Atlassian	This High severity Injection vulnerability was introduced in Assets Discovery 1.0 - 6.2.0 (all versions). Assets Discovery, which can be downloaded via Atlassian Marketplace, is a network scanning tool that can be used with or without an agent with Jira Service Management Cloud, Data Center or Server. It detects hardware and software that is connected to your local network and extracts detailed information	2024-02-20	7.2	High

متاح

		about each asset. This data can then be imported into Assets in Jira Service Management to help you manage all of the devices and configuration items within your local network. This Injection vulnerability, with a CVSS Score of 7.2, allows an authenticated attacker to modify the actions taken by a system call which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Assets Discovery customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions See the release notes (https://confluence.atlassian.com/assetapps/assets-discovery-3-2-1-cloud-6-2-1-data_center-1333987182.html). You can download the latest version of Assets Discovery from the Atlassian Marketplace (https://marketplace.atlassian.com/apps/1214668/assets-discovery?hosting=datacenter&tab=installation). This vulnerability was reported via our Penetration Testing program.			
CVE-2023-6397	Zyxel	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from 4.32 through 5.37 Patch 1 and USG FLEX series firmware versions from 4.50 through 5.37 Patch 1 could allow a LAN-based attacker to cause denial-of-service (DoS) conditions by downloading a crafted RAR compressed file onto a LAN-side host if the firewall has the “Anti-Malware” feature enabled.	2024-02-20	6.5	Medium
CVE-2024-25604	Liferay	Liferay Portal 7.2.0 through 7.4.3.4, and older unsupported versions, and Liferay DXP 7.4.13, 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions does not properly check user permissions, which allows remote authenticated users with the VIEW user permission to edit their own permission via the User and Organizations section of the Control Panel.	2024-02-20	6.5	Medium
CVE-2024-26270	Liferay	The Account Settings page in Liferay Portal 7.4.3.76 through 7.4.3.99, and Liferay DXP 2023.Q3 before patch 5, and 7.4 update 76 through 92 embeds the user’s hashed password in the page’s HTML source, which allows man-in-the-middle attackers to steal a user's hashed password.	2024-02-20	6.5	Medium
CVE-2023-29179	Fortinet	A null pointer dereference in Fortinet FortiOS version 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, Fortiproxy version 7.2.0 through 7.2.4, 7.0.0 through 7.0.10 allows attacker to denial of service via specially crafted HTTP requests.	2024-02-22	6.5	Medium
CVE-2024-22395	SonicWall	Improper access control vulnerability has been identified in the SMA100 SSL-VPN virtual office portal, which in specific conditions could potentially enable a remote authenticated attacker to associate another user's MFA mobile application.	2024-02-24	6.3	Medium
CVE-2023-5190	Liferay	Open redirect vulnerability in the Countries Management’s edit region page in Liferay Portal 7.4.3.45 through 7.4.3.101, and Liferay DXP 2023.Q3 before patch 6, and 7.4 update 45 through 92 allows remote attackers to redirect users to arbitrary external URLs via the _com_liferay_address_web_internal_portlet_CountriesManagementAdminPortlet_redirect parameter.	2024-02-20	6.1	Medium
CVE-2023-44308	Liferay	Open redirect vulnerability in adaptive media administration page in Liferay DXP 2023.Q3 before patch 6, and 7.4 GA through update 92 allows remote attackers to redirect users to arbitrary external URLs via the _com_liferay_adaptive_media_web_portlet_AMPortlet_redirect parameter.	2024-02-20	6.1	Medium
CVE-2024-25608	Liferay	HtmlUtil.escapeRedirect in Liferay Portal 7.2.0 through 7.4.3.18, and older unsupported versions, and Liferay DXP 7.4 before	2024-02-20	6.1	Medium

متـاح

		update 19, 7.3 before update 4, 7.2 before fix pack 19, and older unsupported versions can be circumvented by using the 'REPLACEMENT CHARACTER' (U+FFFD), which allows remote attackers to redirect users to arbitrary external URLs via the (1) 'redirect` parameter (2) `FORWARD_URL` parameter, (3) `noSuchEntryRedirect` parameter, and (4) others parameters that rely on HtmlUtil.escapeRedirect.			
CVE-2024-25609	Liferay	HtmlUtil.escapeRedirect in Liferay Portal 7.2.0 through 7.4.3.12, and older unsupported versions, and Liferay DXP 7.4 before update 9, 7.3 service pack 3, 7.2 fix pack 15 through 18, and older unsupported versions can be circumvented by using two forward slashes, which allows remote attackers to redirect users to arbitrary external URLs via the (1) 'redirect` parameter (2) `FORWARD_URL` parameter, and (3) others parameters that rely on HtmlUtil.escapeRedirect. This vulnerability is the result of an incomplete fix in CVE-2022-28977.	2024-02-20	6.1	Medium
CVE-2023-6399	Zyxel	A format string vulnerability in Zyxel ATP series firmware versions from 4.32 through 5.37 Patch 1, USG FLEX series firmware versions from 4.50 through 5.37 Patch 1, USG FLEX 50(W) series firmware versions from 4.16 through 5.37 Patch 1, USG20(W)-VPN series firmware versions from 4.16 through 5.37 Patch 1, and USG FLEX H series firmware versions from 1.10 through 1.10 Patch 1 could allow an authenticated IPSec VPN user to cause DoS conditions against the “deviceid” daemon by sending a crafted hostname to an affected device if it has the “Device Insight” feature enabled.	2024-02-20	5.7	Medium
CVE-2024-25149	Liferay	Liferay Portal 7.2.0 through 7.4.1, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 15, and older unsupported versions does not properly restrict membership of a child site when the "Limit membership to members of the parent site" option is enabled, which allows remote authenticated users to add users who are not a member of the parent site to a child site. The added user may obtain permission to perform unauthorized actions in the child site.	2024-02-20	5.4	Medium
CVE-2024-25151	Liferay	The Calendar module in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 15, and older unsupported versions does not escape user supplied data in the default notification email template, which allows remote authenticated users to inject arbitrary web script or HTML via the title of a calendar event or the user's name. This may lead to a content spoofing or cross-site scripting (XSS) attacks depending on the capability of the receiver's mail client.	2024-02-21	5.4	Medium
CVE-2023-33843	IBM	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 256544.	2024-02-21	5.4	Medium
CVE-2024-25605	Liferay	The Journal module in Liferay Portal 7.2.0 through 7.4.3.4, and older unsupported versions, and Liferay DXP 7.4.13, 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions grants guest users view permission to web content templates by default, which allows remote attackers to view any template via the UI or API.	2024-02-20	5.3	Medium
CVE-2024-26267	Liferay	In Liferay Portal 7.2.0 through 7.4.3.25, and older unsupported versions, and Liferay DXP 7.4 before update 26, 7.3 before update 5, 7.2 before fix pack 19, and older unsupported versions the default value of the portal property `http.header.version.verbosity` is set to `full`, which allows remote attackers to easily identify the version of the application that is running and the vulnerabilities that affect that version via 'Liferay-Portal` response header.	2024-02-20	5.3	Medium
CVE-2024-26268	Liferay	User enumeration vulnerability in Liferay Portal 7.2.0 through 7.4.3.26, and older unsupported versions, and Liferay DXP 7.4 before update 27, 7.3 before update 8, 7.2 before fix pack 20, and older unsupported versions allows remote attackers to determine if an account exist in the application by comparing the request's response time.	2024-02-20	5.3	Medium
CVE-2024-20325	Cisco	A vulnerability in the Live Data server of Cisco Unified Intelligence Center could allow an unauthenticated, local attacker to read and modify data in a repository that belongs to an internal service on an affected device. This vulnerability is due to insufficient access control implementations on cluster configuration CLI requests. An attacker could exploit this vulnerability by sending a cluster configuration CLI request to specific directories on an affected device. A successful exploit could allow the attacker to read and modify data that is handled by an internal service on the affected device.	2024-02-21	5.1	Medium

متاح

CVE-2024-26265	Liferay	The Image Uploader module in Liferay Portal 7.2.0 through 7.4.3.15, and older unsupported versions, and Liferay DXP 7.4 before update 16, 7.3 before update 4, 7.2 before fix pack 19, and older unsupported versions relies on a request parameter to limit the size of files that can be uploaded, which allows remote authenticated users to upload arbitrarily large files to the system's temp folder by modifying the `maxFileSize` parameter.	2024-02-20	5	Medium
CVE-2024-21423	Microsoft	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2024-02-23	4.8	Medium
CVE-2024-25150	Liferay	Information disclosure vulnerability in the Control Panel in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before update 4, 7.2 before fix pack 19, and older unsupported versions allows remote authenticated users to obtain a user's full name from the page's title by enumerating user screen names.	2024-02-20	4.3	Medium
CVE-2024-26188	Microsoft	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-02-23	4.3	Medium
CVE-2023-50306	IBM	IBM Common Licensing 9.0 could allow a local user to enumerate usernames due to an observable response discrepancy. IBM X-Force ID: 273337.	2024-02-20	4	Medium
CVE-2023-50955	IBM	IBM InfoSphere Information Server 11.7 could allow an authenticated privileged user to obtain the absolute path of the web server installation which could aid in further attacks against the system. IBM X-Force ID: 275777.	2024-02-21	2.4	Low

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

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