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

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٢٤ ديسمبر إلى ٣١ ديسمبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 24th of December to 31st of December. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-51467	apache - ofbiz	The vulnerability permits attackers to circumvent authentication processes, enabling them to remotely execute arbitrary code	2023-12-26	9.8	Critical
CVE-2023-49299	apache - dolphinscheduler	Improper Input Validation vulnerability in Apache DolphinScheduler. An authenticated user can cause arbitrary, unsandboxed javascript to be executed on the server.This issue affects Apache DolphinScheduler: until 3.1.9. Users are recommended to upgrade to version 3.1.9, which fixes the issue.	2023-12-30	8.8	High
CVE-2023-43064	ibm - multiple products	Facsimile Support for IBM i 7.2, 7.3, 7.4, and 7.5 could allow a local user to gain elevated privileges due to an unqualified library call. A malicious actor could cause arbitrary code to run with the privilege of the user invoking the facsimile support. IBM X-Force ID: 267689.	2023-12-25	7.8	High
CVE-2020-17163	microsoft - python_extension	Visual Studio Code Python Extension Remote Code Execution Vulnerability	2023-12-29	7.8	High
CVE-2023-49880	ibm - financial_transaction_manager	In the Message Entry and Repair (MER) facility of IBM Financial Transaction Manager for SWIFT Services 3.2.4 the sending address and the message type of FIN messages are assumed to be immutable. However, an attacker might modify these elements of a business transaction. IBM X-Force ID: 273183.	2023-12-25	7.5	High
CVE-2023-50968	apache - ofbiz	Arbitrary file properties reading vulnerability in Apache Software Foundation Apache OFBiz when user operates an uri call without authorizations. The same uri can be operated to realize a SSRF attack also without authorizations. Users are recommended to upgrade to version 18.12.11, which fixes this issue.	2023-12-26	7.5	High
CVE-2023-3171	redhat - jboss_enterprise_application_platform	A flaw was found in EAP-7 during deserialization of certain classes, which permits instantiation of HashMap and HashTable with no checks on resources consumed. This issue could allow an attacker to submit malicious requests using these classes, which could eventually exhaust the heap and result in a Denial of Service.	2023-12-27	7.5	High
CVE-2023-34829	tp-link - tapo	Incorrect access control in TP-Link Tapo before v3.1.315 allows attackers to access user credentials in plaintext.	2023-12-28	6.5	Medium
CVE-2021-38927	ibm - multiple products	IBM Aspera Console 3.4.0 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	2023-12-25	6.1	Medium

		credentials disclosure within a trusted session. IBM X-Force ID: 210322.			
CVE-2023-50891	zohocorp - zoho_forms	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zoho Forms Form plugin for WordPress – Zoho Forms allows Stored XSS.This issue affects Form plugin for WordPress – Zoho Forms: from n/a through 3.0.1.	2023-12-29	5.4	Medium
CVE-2023-51766	exim - exim	Exim before 4.97.1 allows SMTP smuggling in certain PIPELINING/CHUNKING configurations. Remote attackers can use a published exploitation technique to inject e-mail messages with a spoofed MAIL FROM address, allowing bypass of an SPF protection mechanism. This occurs because Exim supports <LF>.<CR><LF> but some other popular e-mail servers do not.	2023-12-24	4.3	Medium

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.