مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-SAP Products

Tracking #:432315700

Date:14-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that SAP recently released security updates to patch multiple vulnerabilities in its products.

TECHNICAL DETAILS:

On March 12th, 2024 SAP has released security updates that addressed critical vulnerabilities in several of its products, including Business Client, Build Apps, and NetWeaver AS Java. These vulnerabilities could allow attackers to execute unauthorized commands on affected systems, potentially compromising sensitive data and disrupting operations.

Software Updates and Vulnerabilities Details:

Note#	Title	Priority	CVSS
2622660	*Update to Security Note released on April 2018 Patch Day:* Security updates for the browser control Google Chromium delivered with SAP Business Client Product - SAP Business Client, Versions - 6.5, 7.0, 7.70	Hot News	10.0
3425274	[CVE-2019-10744] Code Injection vulnerability in applications built with SAP Build Apps Product - SAP Build Apps, Versions < 4.9.145	Hot News	9.4
3433192	[CVE-2024-22127] Code Injection vulnerability in SAP NetWeaver AS Java (Administrator Log Viewer plug-in) Product - SAP NetWeaver AS Java (Administrator Log Viewer plug-in), Version - 7.50	Hot News	9.1
3346500	*Update to Security Note released on August 2023 Patch Day:* [CVE-2023-39439] Improper authentication in SAP Commerce Cloud Product - SAP Commerce, Versions – HY_COM 2105, HY_COM 2205, COM_CLOUD 2211	High	8.8
3410615	[CVE-2023-44487] Denial of service (DOS) in SAP HANA XS Classic and HANA XS Advanced Product- SAP HANA Database, Version – 2.0 Product- SAP HANA Extended Application Services Advanced (XS Advanced), Version – 1.0	High	7.5
3414195	[CVE-2023-50164] Path Traversal Vulnerability in SAP BusinessObjects Business Intelligence Platform (Central Management Console) Product - SAP BusinessObjects Business Intelligence Platform (Central Management Console), Versions - 4.3	High	7.2

Note#	Title	Priority	CVSS
3377979	[CVE-2024-27902] Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS ABAP, applications based on SAPGUI for HTML (WebGUI) Product – SAP NetWeaver AS ABAP applications based on SAPGUI for HTML (WebGUI), Versions – 7.89, 7.93	Medium	5.4
3425682	[CVE-2024-25644] Information Disclosure vulnerability in SAP NetWeaver (WSRM) Product - NetWeaver (WSRM), Versions – 7.50	Medium	5.3
3428847	[CVE-2024-25645] Information Disclosure vulnerability in SAP NetWeaver (Enterprise Portal) Product - SAP NetWeaver (Enterprise Portal), Version – 7.50	Medium	5.3
3434192	[CVE-2024-28163] Information Disclosure vulnerability in SAP NetWeaver Process Integration (Support Web Pages) Product - SAP NetWeaver Process Integration (Support Web Pages), Versions – 7.50	Medium	5.3
3417399	[CVE-2024-22133] Improper Access Control in SAP Fiori Front End Server Product – SAP Fiori Front End Server, Version – 605	Medium	4.6
3419022	[CVE-2024-27900] Missing Authorization check in SAP ABAP Platform Product - SAP ABAP Platform, Versions – 758, 795	Medium	4.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by SAP.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://support.sap.com/en/my-support/knowledge-base/security-notes-news/march-2024.html