مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-SAP Products

Tracking #:432315784

Date:24-04-2024

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

SAP recently released security updates to address vulnerabilities in various SAP products. These vulnerabilities could allow attackers to gain unauthorized access to data, cause denial-of-service (DoS) conditions, or execute arbitrary code on affected systems.

Software Updates and Vulnerabilities Details:

Description	Severity	CVSS
[CVE-2024-27899] Security misconfiguration vulnerability in SAP NetWeaver AS Java User Management Engine Product - SAP NetWeaver AS Java User Management Engine, Versions - SERVERCORE 7.50, J2EE-APPS 7.50, UMEADMIN 7.50	High	8.8
[CVE-2024-25646] Information Disclosure vulnerability in SAP BusinessObjects Web Intelligence Product - SAP BusinessObjects Web Intelligence, Versions - 4.2, 4.3	High	7.7
[CVE-2024-27901] Directory Traversal vulnerability in SAP Asset Accounting Product- SAP Asset Accounting, Versions - SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_FIN617, SAP_FIN 618, SAP_FIN700	High	7.2
Stack overflow vulnerability on the component images of SAP Integration Suite (EDGE INTEGRATION CELL) Product - SAP Edge Integration Cell, Versions older than 8.13.5	Medium	6.8
[CVE-2024-30218] Denial of service (DOS) vulnerability in SAP NetWeaver AS ABAP and ABAP Platform Product - SAP NetWeaver AS ABAP and ABAP Platform, Versions - KRNL64NUC 7.22, KRNL64NUC 7.22EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KERNEL 7.22, KERNEL 7.53, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.93	Medium	6.5
[CVE-2024-28167] Missing Authorization check in SAP Group Reporting Data Collection (Enter Package Data) Product - SAP Group Reporting Data Collection (Enter Package Data), Versions - S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108, SAP_GRDC_CLOUD 1.0.0	Medium	6.5
[CVE-2022-29613] Information Disclosure vulnerability in SAP Employee Self Service(Fiori My Leave Request) Product - SAP Employee Self Service (Fiori My Leave Request), Version - 605	Medium	6.5
[CVE-2023-40306] URL Redirection vulnerability in SAP S/4HANA (Manage Catalog Items and Cross-Catalog search) Product - SAP S/4HANA (Manage Catalog Items and Cross-Catalog search), Versions – S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106	Medium	6.1

Description	Severity	CVSS
[CVE-2024-27898] Server-Side Request Forgery in SAP NetWeaver (tc~esi~esp~grmg~wshealthcheck~ear) Product - SAP NetWeaver, Version - 7.50	Medium	5.3
[Multiple CVEs] Cross-Site Scripting (XSS) vulnerabilities in SAP Business Connector CVEs - CVE-2024-30214, CVE-2024-30215 Product - SAP Business Connector, Version - 4.8	Medium	4.8
[CVE-2024-30216] Missing Authorization check in SAP S/4 HANA (Cash Management) Product – SAP S/4 HANA (Cash Management), Versions – S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108	Medium	4.3
[CVE-2024-30217] Missing Authorization check in SAP S/4 HANA (Cash Management) Product - SAP S/4 HANA (Cash Management), Versions – S4CORE 106, S4CORE 107, S4CORE 108	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/april-2024.html