مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- SAP

Tracking #:432316376

Date:09-10-2024

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

On October 8, 2024, SAP released security updates to address multiple vulnerabilities in its products. These vulnerabilities could potentially allow attackers to gain unauthorized access, execute malicious code, or steal sensitive data.

Description	Severity	CVSS
Update to Security Note released on August 2024 Patch Day: [CVE-2024-41730] Missing Authentication check in SAP BusinessObjects Business Intelligence Platform Product - SAP BusinessObjects Business Intelligence Platform, Versions - ENTERPRISE 420, 430, 440	Critical	9.8
[CVE-2022-23302] Multiple vulnerabilities in SAP Enterprise Project Connection Related CVEs - CVE-2024-22259, CVE-2024-38809, CVE-2024-38808 Product - SAP Enterprise Project Connection, Version - 3.0	High	8.0
[CVE-2024-37179] Insecure File Operations vulnerability in SAP BusinessObjects Business Intelligence Platform (Web Intelligence) Product - SAP BusinessObjects Business Intelligence Platform (Web Intelligence), Version - ENTERPRISE 420, 430, 2025, ENTERPRISECLIENTTOOLS 420, 430, 2025	High	7.7
Update to Security Note released on July 2024 Patch Day: [CVE-2024-39592] Missing Authorization check in SAP PDCE Product- SAP PDCE, Versions - S4CORE 102, 103, S4COREOP 104, 105, 106, 107, 108	High	7.7
Update to Security Note released on September 2024 Patch Day [CVE-2024-45283] Information disclosure vulnerability in SAP NetWeaver AS for Java (Destination Service) Product - SAP NetWeaver AS for Java (Destination Service), Versions - 7.50	Medium	6.0
[CVE-2024-45278] Cross-Site Scripting (XSS) vulnerability in SAP Commerce Backoffice Product - SAP Commerce Backoffice, Versions - HY_COM 2205, COM_CLOUD 2211	Medium	5.4
[CVE-2024-47594] Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal (KMC) Product - SAP NetWeaver Enterprise Portal (KMC), Version - KMC-BC 7.5	Medium	5.4

Description	Severity	CVSS
[CVE-2024-45277] Prototype Pollution vulnerability in SAP HANA Client Product - SAP HANA Client, Version - HDB_CLIENT 2.0	Medium	4.3
[CVE-2024-45282] HTTP Verb Tampering in SAP S/4 HANA(Manage Bank Statements) Product - SAP S/4 HANA (Manage Bank Statements), Versions – S4CORE, 102, 103, 104, 105, 106, 107	Medium	4.3
Update to Security Note released on September 2024 Patch Day: [CVE-2024-41729] Information Disclosure vulnerability in the SAP NetWeaver BW (BEx Analyzer) Product- SAP NetWeaver BW (BEx Analyzer), Versions – DW4CORE 200, DW4CORE 300, DW4CORE 400, SAP_BW 700, SAP_BW 701, SAP_BW 702, SAP_BW 731, SAP_BW 740, SAP_BW 750, SAP_BW 751, SAP_BW 752, SAP_BW 753, SAP_BW 754, SAP_BW 755, SAP_BW 756, SAP_BW 757, SAP_BW 758	Medium	4.3
Update to Security Note released on August 2024 Patch Day: [CVE-2024-42373] Missing Authorization Check in SAP Student Life Cycle Management (SLcM) Product - SAP Student Life Cycle Management (SLcM), Versions – IS-PS-CA 617, 618, 802, 803, 804, 805, 806, 807, 808	Medium	4.3
Update to Security Note released on July 2024 Patch Day: [CVE-2024-37180] Information Disclosure vulnerability in SAP NetWeaver Application Server for ABAP and ABAP Platform Product - SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions - SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758	Medium	4.1

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/october-2024.html