مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-SAP Products

Tracking #:432315900

Date:28-05-2024

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 released its May 2024 security updates to address vulnerabilities in various SAP products. These vulnerabilities could be exploited by attackers to gain unauthorized access to SAP systems, steal sensitive data, or disrupt business operations.

Vulnerabilities Details:

Description	Severity	CVSS
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	Critical	10.0
[CVE-2019-17495] Multiple vulnerabilities in SAP CX Commerce Related CVE - CVE-2022-36364 Product- SAP Commerce, Version - HY_COM 2205	Critical	9.8
[CVE-2024-33006] File upload vulnerability in SAP NetWeaver Application Server ABAP and ABAP Platform Product- SAP NetWeaver Application Server 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	Critical	9.6
[CVE-2024-28165] Cross site scripting vulnerability in SAP BusinessObjects Business Intelligence Platform Product- SAP BusinessObjects (Business Intelligence Platform), Versions – 430, 440	High	8.1
[CVE-2024-32730] Missing authorization check in SAP Enable Now Manager Product- SAP Enable Now, Version - 1704	Medium	6.5
[CVE-2024-34687] Cross-Site Scripting (XSS) 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, SAP_BASIS 795, SAP_BASIS 796	Medium	6.5
[CVE-2024-32733] Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Application Server ABAP and ABAP Platform Product- SAP NetWeaver Application Server ABAP and ABAP Platform, Versions - 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	6.1
[CVE-2024-33002] Cross-Site Scripting (XSS) Vulnerability in SAP S/4HANA (Document Service Handler for DPS) Product - SAP S/4HANA (Document Service Handler for DPS), Versions – SAP_BASIS 740, SAP_BASIS 750	Medium	6.1
[CVE-2024-32731] Missing Authorization check in SAP My Travel Requests Product- My Travel Requests, Version – 600	Medium	5.5

Description	Severity	CVSS
Update to Security Note released on May 2021 Patch Day: Information Disclosure in Enterprise Services Repository of SAP Process Integration Product - SAP Process Integration, Versions - MESSAGING 7.31, MESSAGING 7.40, MESSAGING 7.50, NWCEIDE 7.31, SAP_XIESR 7.31, SAP_XIESR 7.40, SAP_XIESR 7.50, SAP_XITOOL 7.31, SAP_XITOOL 7.40, SAP_XITOOL 7.50, SAP_XIAF 7.31, SAP_XIAF 7.40, SAP_XIAF 7.50, SAP_XIGUILIB 7.31, SAP_XIGUILIB 7.40, SAP_XIGUILIB 7.50	Medium	5.3
[CVE-2024-33008] Memory Corruption vulnerability in SAP Replication Server Product – SAP Replication Server, Versions – 16.0, 16.0.3, 16.0.4	Medium	4.9
[Multiple CVEs] Missing Authorization Checks in SAP S/4 HANA (Manage Bank Statement Reprocessing Rules) CVEs - CVE-2024-4139, CVE-2024-4138 Product – SAP S/4 HANA (Manage Bank Statement Reprocessing Rules), Versions – SAPSCORE 131, S4CORE 105, S4CORE 106, S4CORE107, S4CORE 108	Medium	4.3
[CVE-2024-33004] Insecure Storage vulnerability in SAP BusinessObjects Business Intelligence Platform (Webservices) Product – SAP BusinessObjects Business Intelligence Platform (Webservices), Versions – 430, 440	Medium	4.3
Update to Security Note released on December 2017 Patch Day: Potential information disclosure relating to PI Integration Directory Product - SAP Process Integration, Versions - MESSAGING 7.10, MESSAGING 7.11, MESSAGING 7.30, MESSAGING 7.31, MESSAGING 7.40, MESSAGING 7.50, NWCEIDE 7.31, SAP_XITOOL 7.00, SAP_XITOOL 7.01, SAP_XITOOL 7.02, SAP_XITOOL 7.10, SAP_XITOOL 7.11, SAP_XITOOL 7.30, SAP_XITOOL 7.31, SAP_XITOOL 7.40, SAP_XITOOL 7.50, SAP_XIAF 7.31, SAP_XIAF 7.40, SAP_XIAF 7.50, SAP_XIPCK 7.00, SAP_XIPCK 7.01, SAP_XIPCK 7.02, SAP_XIPCK 7.10, SAP_XIPCK 7.11, SAP_XIPCK 7.30	Medium	4.3
[CVE-2024-33009] SQL injection vulnerability in SAP Global Label Management (GLM) Product – SAP Global Label Management (GLM), Versions – 605, 606, 616, 617	Low	3.7
[CVE-2024-33000] Missing Authorization check in SAP Bank Account Management Product – SAP Bank Account Management, Versions – 100, 101, 102, 103, 104, 105, 106, 107, 108	Low	3.5
[CVE-2024-33007] Client-side script execution vulnerability in SAP UI5(PDFViewer) Product - SAPUI5, Versions – 754, 755, 756, 757, 758	Low	3.5

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/may-2024.html