مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

SAP Security Updates

Tracking #:432316612

Date:10-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SAP released its monthly Security Patch Day updates, addressing several vulnerabilities across various SAP products.

TECHNICAL DETAILS:

SAP released its monthly Security Patch Day updates, addressing several vulnerabilities across various SAP products, including SAP NetWeaver AS, SAP BusinessObjects Business Intelligence Platform, SAP Commerce Cloud, SAP Web Dispatcher, and more. This update includes 10 new Security Notes addressing various vulnerabilities across SAP products. Additionally, 3 previously released Security Notes were updated to reflect newly discovered information or improvements.

Critical and High-Priority Vulnerabilities:

1. CVE-2024-47578 Multiple Vulnerabilities in SAP NetWeaver AS for JAVA (Adobe Document Services)
   - CVSS Score: 9.1 (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)
   - Affected Component: SAP NetWeaver AS for JAVA (Adobe Document Services)
   - Description: A set of vulnerabilities that can compromise sensitive information and severely impact system integrity and availability.
   - Priority: HotNews
   - Action Required: Immediate patching is critical as attackers with administrative privileges (PR:H) can exploit these vulnerabilities to access sensitive data or disrupt SAP systems.

2. CVE-2024-47590 Cross-Site Scripting (XSS) in SAP Web Dispatcher
   - CVSS Score: 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
   - Affected Component: SAP Web Dispatcher
   - Description: A high-severity XSS vulnerability that allows attackers to inject malicious code into the web interface, potentially enabling session hijacking and content spoofing.
   - Priority: Correction with high priority
   - Action Required: Immediate patching is essential, as this vulnerability is exploitable without prior authentication (PR:N), which increases the urgency.

3. CVE-2024-47586 NULL Pointer Dereference in SAP NetWeaver AS ABAP and ABAP Platform
   - CVSS Score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
   - Affected Component: SAP NetWeaver AS ABAP
   - Description: This vulnerability can lead to a denial-of-service (DoS), causing the system to become unavailable.
   - Priority: Correction with high priority
   - Action Required: Apply the patch immediately to prevent service disruptions.

4. CVE-2024-54197 Server-Side Request Forgery (SSRF) in SAP NetWeaver Administrator (System Overview)
   - CVSS Score: 7.2 (AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N)
   - Affected Component: SAP NetWeaver Administrator

- Description: SSRF vulnerabilities allow unauthenticated attackers to access internal resources, potentially exposing sensitive data or leveraging trusted connections.
- Priority: Correction with high priority
- Action Required: Patching is critical to prevent exploitation of this vulnerability, which may give attackers access to internal SAP resources.

5. CVE-2024-54198 Information Disclosure via RFC in SAP NetWeaver Application Server ABAP
   - CVSS Score: 8.5 (AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H)
   - Affected Component: SAP NetWeaver AS ABAP
   - Description: This high-risk vulnerability allows attackers with low privileges (PR:L) to access critical information or compromise system integrity by exploiting complex scenarios.
   - Priority: Correction with high priority
   - Action Required: Immediate patching is required to prevent unauthorized access to sensitive data.

RECOMMENDATIONS:

- Organizations are strongly advised to assess and apply the new Security Notes and updates as soon as possible to protect their SAP environments from exploitation.

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/december-2024.html