



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates – SAP Products**

Tracking #:432316146

Date:14-08-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that SAP released a security bulletin addressing multiple vulnerabilities including critical vulnerabilities.

## TECHNICAL DETAILS:

### Vulnerability Details:

- **CVE-2024-41730** | CVSS Score: 9.8 – **Critical** | Missing Authentication check in SAP BusinessObjects Business Intelligence Platform
  - If Single Signed On is enabled on Enterprise authentication, an unauthorized user can get a logon token using a REST endpoint. The attacker can fully compromise the system resulting in High impact on confidentiality, integrity and availability.
  - Affected Products - SAP BusinessObjects Business Intelligence Platform, Version – ENTERPRISE 430, 440
- **CVE-2024-29415** | CVSS Score: 9.1 – **Critical** | Server-Side Request Forgery vulnerability in applications built with SAP Build Apps
  - The ip package through 2.0.1 for Node.js might allow SSRF because some IP addresses are improperly categorized as globally routable via isPublic.
  - Affected Products - SAP Build Apps, Versions < 4.11.130
- **CVE-2024-42374** | CVSS Score: 8.2 – High | XML injection in SAP BEx Web Java Runtime Export Web Service
  - BEx Web Java Runtime Export Web Service does not sufficiently validate an XML document accepted from an untrusted source. An attacker can retrieve information from the SAP ADS system and exhaust the number of XMLForm service which makes the SAP ADS rendering (PDF creation) unavailable.
  - Affected Products- SAP BEx Web Java Runtime Export Web Service, Versions - BI-BASE-E 7.5, BI-BASE-B 7.5, BI-IBC 7.5, BI-BASE-S 7.5, BIWEBAPP 7.5

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates 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/august-2024.html>