Authentication Bypass Vulnerability in SAP

Severity Level: High
Components Affected

- SAP BusinessObjects Business Intelligence Platform version 430
- SAP BusinessObjects Business Intelligence Platform version 440

Overview

SAP released a security advisory for a critical authentication bypass vulnerability, CVE-2024-41730, in SAP BusinessObjects Business Intelligence Platform. This flaw allows remote attackers to bypass authentication mechanisms, potentially leading to full system compromise.

Description

CVE-2024-41730 is a “missing authentication check” vulnerability. If Single Sign-On is enabled for Enterprise authentication, an attacker can exploit a REST endpoint to obtain a logon token and compromise the system entirely, affecting confidentiality, integrity, and availability.

Impact

- Authentication Bypass
- Privilege escalation

Solution/ Workarounds

Before installation of the software, please visit the software vendor website for more details.

Apply fixes issued by the vendor:

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2024.html

Reference

- https://www.bleepingcomputer.com/news/security/critical-sap-flaw-allows-remote-attackers-to-bypass-authentication/

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.