

Security Advisory 2024-079

# Critical SAP Authentication Bypass Vulnerability

August 14, 2024 — v1.0

**TLP:CLEAR**

*History:*

- 14/08/2024 — v1.0 – Initial publication

## Summary

On August 13, 2024, SAP released a security advisory [1] 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. The vulnerability has a CVSS score of 9.8, highlighting its severity.

## Technical Details

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 [1,2].

## Affected Products

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

## Recommendations

CERT-EU strongly advises applying the security patches provided by SAP immediately to mitigate this critical vulnerability.

## References

- [1] <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2024.html>
- [2] <https://www.bleepingcomputer.com/news/security/critical-sap-flaw-allows-remote-attackers-to-bypass-authentication/>