BEACON LAB CSIRT

CYBOLT

Alert Bulletin

Bulletin N.: 2024-48

Publication Date: 10/10/2024

Subject: Alert 2024-48: Critical Remote Code Execution Vulnerability in SAP Business Intelligence Platform

Traffic Light Protocol (TLP): White

This month, SAP fixed a critical vulnerability in its BusinessObjects platform, identified as CVE-2024-41730. The vulnerability affects the SAP BusinessObjects Business Intelligence Platform, allowing an unauthenticated attacker to perform unsafe data deserialization attacks. This vulnerability is particularly dangerous as it can lead to remote code execution (RCE) on the affected server, compromising the confidentiality, integrity, and availability of critical information handled by the platform.

The vulnerability has a CVSS score of 9.8, classifying it as critical, and affects SAP BusinessObjects BI Platform versions 420 and 430. To exploit this flaw, attackers can send a malicious request to the server, potentially enabling them to execute arbitrary code and take control of the system.

To address the CVE-2024-41730 vulnerability in SAP BusinessObjects Business Intelligence Platform, SAP has released security patches that should be applied to the affected versions. The patches are available on the SAP Support Portal, where they can be downloaded and implemented following the update guides provided by SAP at the following link:

[SAP Security Patch Day – October 2024]