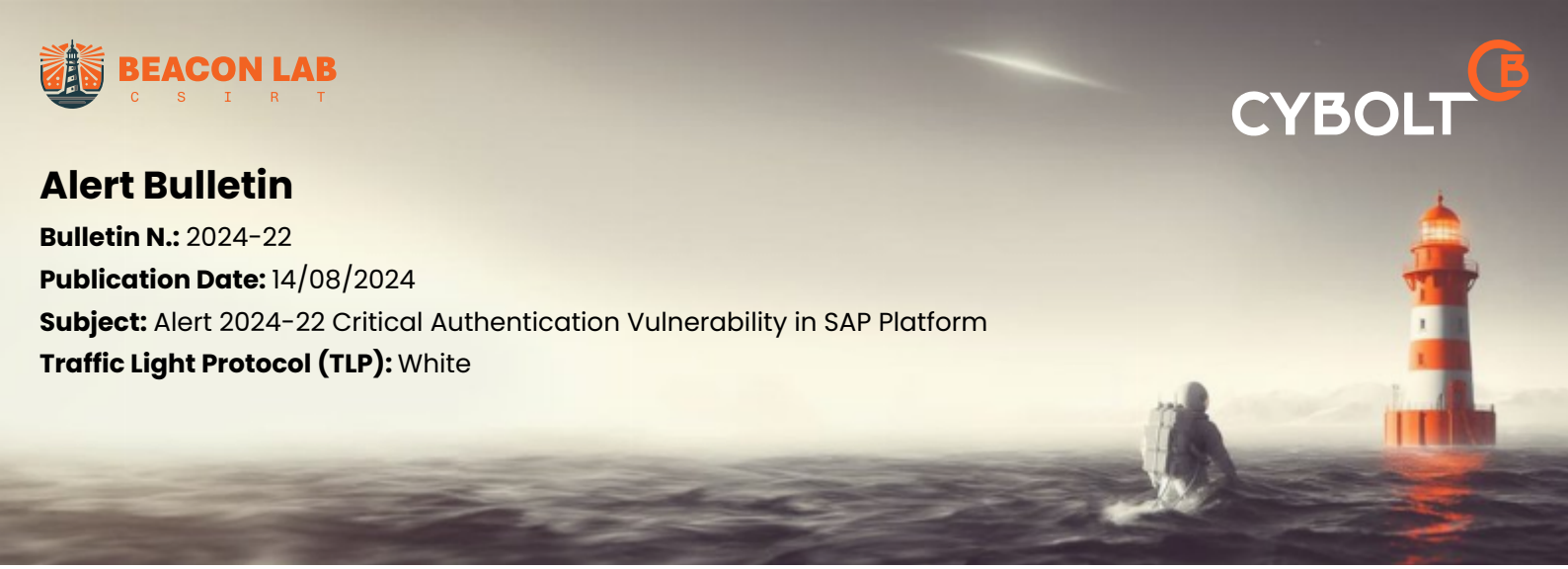

Alert Bulletin

Bulletin N.: 2024-22
Publication Date: 14/08/2024
Subject: Alert 2024-22 Critical Authentication Vulnerability in SAP Platform
Traffic Light Protocol (TLP): White

Affected Product(s):

- **BusinessObjects Business Intelligence** versions **430** and **440**

Description:

SAP has released its **August 2024** security patch package, addressing **17 vulnerabilities**, including a critical authentication omission that could allow remote attackers to fully compromise the system.

Among the most significant vulnerabilities is **CVE-2024-41730**, which has been rated with a score of **9.8** on the **CVSS v3.1** scale. This "missing authentication check" flaw affects versions **430** and **440** of the **SAP BusinessObjects Business Intelligence Platform** and is exploitable under certain conditions.

In the **SAP BusinessObjects Business Intelligence Platform**, if **Single Sign-On (SSO)** is enabled in business authentication, an unauthorized user could obtain a login token through a **REST endpoint**. This would allow the attacker to fully compromise the system, severely impacting the confidentiality, integrity, and availability of business intelligence data and services.

Currently, this vulnerability is under analysis, and not all information is available.

Solution:

Patches are available for the following versions:

- **SBOP BI 4.3 Servers** – Patch Level **SP005**
- **SBOP BI 2025 Servers** – Patch Level **SP00**
- **SBOP BI 4.3 Servers** – Patch Level **SP004**