

Department of the Environment, Climate & Communications

---



## NCSC Alert

---

### Critical vulnerability in SAP BusinessObjects Business Intelligence Platform (CVE-2024-41730, CVSSv3: 9.8)

Thursday 10<sup>th</sup> October, 2024

**STATUS:** **TLP-CLEAR**

*Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP-CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP-CLEAR** information may be shared without restriction.*

For more information on the Traffic Light Protocol, see <https://www.first.org/tp/>.

Please treat this document in accordance with the TLP assigned.

## Description

**Published:** 2024-08-13T04:15:00

**Vendor:** SAP

**Product:** SAP BusinessObjects Business Intelligence Platform;

**CVE ID:** CVE-2024-41730

**CVSS3.x Score<sup>1</sup>:** 9.8

**EPSS<sup>2</sup>:** 0.397000000

(For up to date EPSS score, see here: <https://api.first.org/data/v1/epss?cve=CVE-2024-41730>)

**Summary:** SAP have released a security advisory for a critical authentication bypass vulnerability tracked as [CVE-2024-41730](#). 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.

## Products Affected

SAP BusinessObjects Business Intelligence Platform

- Version – ENTERPRISE 430, 440

## Impact

**Common Weakness Enumeration (CWE)<sup>3</sup>:** CWE-862: Missing Authorisation

**Present in CISA Known Exploited Vulnerability(KEV)<sup>4</sup> catalog:** NO

**Used by Ransomware Operators:** Not Known

## Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from SAP.

Additional recommendations and mitigation's for CVE-2024-41730 can be found in the respective link below:

<https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2024.html> (SAP Account Login Required)

<sup>1</sup><https://www.first.org/cvss/v3.0/specification-document>

<sup>2</sup>[https://www.first.org/epss/articles/prob\\_percentile\\_bins](https://www.first.org/epss/articles/prob_percentile_bins)

<sup>3</sup><https://cwe.mitre.org/>

<sup>4</sup><https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

**DISCLAIMER:** This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre  
Tom Johnson House,  
Beggars Bush,  
Dublin, D04 K7X4,  
Ireland  
**Tel:** +353 (0)1 6782333  
**Mail:** [certreport@ncsc.gov.ie](mailto:certreport@ncsc.gov.ie)  
**Web:** [ncsc.gov.ie](http://ncsc.gov.ie)  
**Twitter:** [ncsc\\_gov\\_ie](https://twitter.com/ncsc_gov_ie)  
**LinkedIn:** [ncsc-ie](https://www.linkedin.com/company/ncsc-ie)



An Láirionad Náisiúnta  
Cibearshlándála  
National Cyber Security Centre