



Insecure Session Management vulnerability in SAP BusinessObjects Business Intelligence Platform

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-24318
State	PUBLISHED
Assigner	sap
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 00:16:04 UTC
Updated	2026-04-14 00:16:04 UTC
Description	Due to an Insecure session management vulnerability in SAP Business Objects Business Intelligence Platform, an unauth

Risk And Classification

Primary CVSS: v3.1 4.2 MEDIUM from cna@sap.com

CVSS: 3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N

Problem Types: CWE-539 | CWE-539 CWE-539: Use of Persistent Cookies Containing Sensitive Information

Version	Source	Type	Score	Severity	Vector
3.1	cna@sap.com	Primary	4.2	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	4.2	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SAP SE	SAP BusinessObjects Business Intelligence Platform	affected ENTERPRISE 430	Not specified
CNA	SAP SE	SAP BusinessObjects Business Intelligence Platform	affected 2025	Not specified
CNA	SAP SE	SAP BusinessObjects Business Intelligence Platform	affected 2027	Not specified

References

Reference	Source	Link	Tags
url.sap/sapsecuritypatchday	cna@sap.com	url.sap	
me.sap.com/notes/3702191	cna@sap.com	me.sap.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report