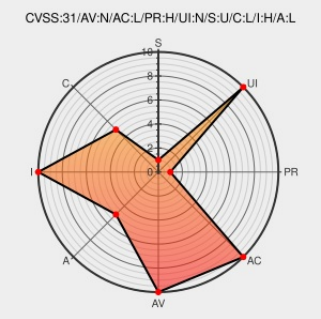
CVE-2022-31596

Published on: Not Yet Published

Last Modified on: 12/13/2022 05:59:00 PM UTC

CVE-2022-31596

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Business Objects Business Intelligence Platform from Sap contain the following vulnerability:

Under certain conditions, an attacker authenticated as a CMS administrator and with high privileges access to the Network in SAP BusinessObjects Business Intelligence Platform (Monitoring DB) - version 430, can access BOE Monitoring database to retrieve and modify (non-personal) system data which would otherwise be restricted. Also, a potential attack could be used to leave the CMS's scope and impact the database. A successful attack could have a low impact on confidentiality, a high impact on integrity, and a low impact on availability.

CVE-2022-31596 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SAP** - **SAP Business Objects Platform (Monitoring DB)** version **= 430**

CVSS3 Score: 6 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	HIGH	LOW

CVE References

Description	Tags	Link
No Description Provided	launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/3213507
Access Denied	www.sap.com text/html Inactive Link Not Archived	MISC www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Under certain conditions, an attacker authenticated as a CMS administrator and with high privileges access to the Net…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Business Objects Business Intelligence Platform	430	All	All	All

cpe:2.3:a:sap:business_objects_business_intelligence_platform:430:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31596 : Under certain conditions, an attacker authenticated as a CMS administrator and with high privilege… twitter.com/i/web/status/1…	2022-12-12 04:07:18
/r/netcve	CVE-2022-31596	2022-12-12 05:40:04

← Previous ID

Next ID→