



CVE-2021-40500

Published on: 10/12/2021 12:00:00 AM UTC

Last Modified on: 10/18/2021 06:21:00 PM UTC

CVE-2021-40500

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Businessobjects Business Intelligence Platform](#) from [Sap](#) contain the following vulnerability:

SAP BusinessObjects Business Intelligence Platform (Crystal Reports) - versions 420, 430, allows an unauthenticated attacker to exploit missing XML validations at endpoints to read sensitive data. These endpoints are normally exposed over the network and successful exploitation can enable the attacker to retrieve arbitrary files from the

server.

CVE-2021-40500 has been assigned by [cna@sap.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [SAP SE](#) - [SAP BusinessObjects Business Intelligence Platform \(Crystal Reports\)](#) version 420

Affected Vendor/Software: [SAP SE](#) - [SAP BusinessObjects Business Intelligence Platform \(Crystal Reports\)](#) version 430

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
SAP Security Patch Day – October 2021 - Product Security Response at SAP - Community Wiki	wiki.scn.sap.com text/html	<input type="checkbox"/> MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=587169983

No Description Provided	launchpad.support.sap.com text/html	<input checked="" type="checkbox"/> MISC launchpad.support.sap.com/#/notes/3074693
--------------------------------	--	---

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Businessobjects Business Intelligence Platform	4.20	All	All	All
Application	Sap	Businessobjects Business Intelligence Platform	4.30	All	All	All

cpe:2.3:a:sap:businessobjects_business_intelligence_platform:4.20:*:*:*:*:*:

cpe:2.3:a:sap:businessobjects_business_intelligence_platform:4.30:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-40500 : #SAP BusinessObjects Business Intelligence Platform Crystal Reports - versions 420, 430, allows... twitter.com/i/web/status/1...	2021-10-12 14:45:12

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022 |

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](#).

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