

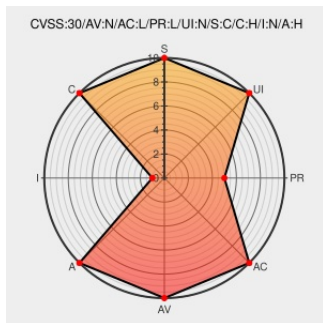


CVE-2020-26831

Published on: 12/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:56 PM UTC

CVE-2020-26831

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

SAP BusinessObjects BI Platform (Crystal Report), versions - 4.1, 4.2, 4.3, does not sufficiently validate uploaded XML entities during crystal report generation due to missing XML validation, An attacker with basic privileges can inject some arbitrary XML entities leading to internal file disclosure, internal directories disclosure, Server-Side Request Forgery (SSRF) and denial-of-service (DoS).

CVE-2020-26831 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP BusinessObjects BI Platform (Crystal Report)** version **4.1**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP BusinessObjects BI Platform (Crystal Report)** version **4.2**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP BusinessObjects BI Platform (Crystal Report)** version **4.3**

CVSS3 Score: **9.6 - CRITICAL**

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

CVSS2 Score: **5.5 - MEDIUM**

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

CVE References

Description

Tags

Link

No Description Provided

Permissions Required

launchpad.support.sap.com

text/html

 MISC

launchpad.support.sap.com/#/notes/2989075

SAP Security Patch Day – December 2020 - Product Security Response at SAP - Community Wiki

Vendor Advisory

wiki.scn.sap.com

text/html

 MISC

wiki.scn.sap.com/wiki/pages/viewpage.action?pagelId=564757079

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	4.1	-	All	All
Application	Sap	Businessobjects Business Intelligence Platform	4.2	-	All	All
Application	Sap	Businessobjects Business Intelligence Platform	4.3	All	All	All
Application	Sap	Businessobjects Business Intelligence Platform	4.1	-	All	All
Application	Sap	Businessobjects Business Intelligence Platform	4.2	-	All	All
Application	Sap	Businessobjects Business Intelligence Platform	4.3	All	All	All

cpe:2.3:a:sap:businessobjects_business_intelligence_platform:4.1:-:*:*:*:*:*:

cpe:2.3:a:sap:businessobjects_business_intelligence_platform:4.2:-:*:*:*:*:*:

cpe:2.3:a:sap:businessobjects_business_intelligence_platform:4.3:*:*:*:*:*:*:

cpe:2.3:a:sap:businessobjects_business_intelligence_platform:4.1:-:*:*:*:*:*:

cpe:2.3:a:sap:businessobjects_business_intelligence_platform:4.2:-:*:*:*:*:*:

cpe:2.3:a:sap:businessobjects_business_intelligence_platform:4.3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)