



CVE-2020-36640

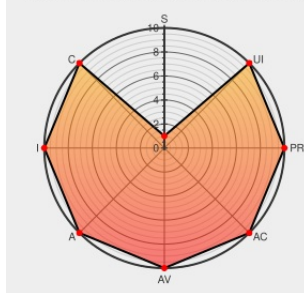
Published on: Not Yet Published

Last Modified on: 11/07/2023 03:22:00 AM UTC

CVE-2020-36640

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Webservice Connector](#) from [Bonitasoft](#) contain the following vulnerability:

A vulnerability, which was classified as problematic, was found in bonitasoft bonita-connector-webservice up to 1.3.0. This affects the function TransformerConfigurationException of the file src/main/java/org/bonitasoft/connectors/ws/SecureWSConnector.java. The manipulation leads to xml external entity reference. Upgrading to version 1.3.1 is able to address this issue. The patch is named a12ad691c05af19e9061d7949b6b828ce48815d5. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217443.

CVE-2020-36640 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **bonitasoft** - **bonita-connector-webservice** version = 1.0

Affected Vendor/Software: **bonitasoft** - **bonita-connector-webservice** version = 1.1

Affected Vendor/Software: **bonitasoft** - **bonita-connector-webservice** version = 1.2

Affected Vendor/Software: **bonitasoft** - **bonita-connector-webservice** version = 1.3

CVSS3 Score: **9.8 - CRITICAL**

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

CVE References

Description	Tags	Link
Release Release 1.3.1 ·	github.com	MISC github.com/bonitasoft/bonita-connector-

bonitasoft/bonita-connector-webservice · GitHub

text/html

webservice/releases/tag/1.3.1

vuldb.com

text/plain

Inactive Link

Not Archived

MISC vuldb.com/?ctiid.217443

fix(vulnerabilities): fix XXE attacks vulnerabilities and other code smell by alachambre · Pull Request #17 · bonitasoft/bonita-connector-webservice · GitHub

github.com

text/html

MISC github.com/bonitasoft/bonita-connector-webservice/pull/17

fix(vulnerabilities): fix XXE attacks vulnerabilities and other code ... · bonitasoft/bonita-connector-webservice@a12ad69 · GitHub

github.com

text/html

MISC github.com/bonitasoft/bonita-connector-webservice/commit/a12ad691c05af19e9061d7949b6b828ce48815d5

vuldb.com

text/plain

Inactive Link

Not Archived

MISC vuldb.com/?id.217443

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

A vulnerability, which was classified as problematic, was found in bonitasoft bonita-connector-webservice up to 1.3.0...

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Bonitasoft	Webservice Connector	All	All	All	All
cpe:2.3:a:bonitasoft:webservice_connector:*****:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 /r/netcve	CVE-2020-36640	2023-01-05 10:38:02

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](#)