



CVE-2020-8441

Published on: 02/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:59 PM UTC

CVE-2020-8441

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

Certain versions of [Jyaml](#) from [Jyaml Project](#) contain the following vulnerability:

JYaml through 1.3 allows remote code execution during deserialization of a malicious payload through the load() function. NOTE: this is a discontinued product.

CVE-2020-8441 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
JYaml / Bugs	Third Party Advisory sourceforge.net text/html	MISC sourceforge.net/p/jyaml/bugs/
CVE-2020-8441 JYaml Vulnerability in NetApp	security.netapp.com	CONFIRM security.netapp.com/advisory/ntap-20200313-

Products NetApp Product Security	text/html	0001/
jyaml Java library - 1.3 Deserialization attack · GitHub	Exploit Third Party Advisory gist.github.com text/html	MISC gist.github.com/j0lt-github/f5141abcacae63d434ecae211422153a
marshalsec/marshalsec.pdf at master · mbechler/marshalsec · GitHub	Technical Description Third Party Advisory github.com text/html	MISC github.com/mbechler/marshalsec/blob/master/marshalsec.pdf
GitHub - mbechler/marshalsec	Third Party Advisory github.com text/html	MISC github.com/mbechler/marshalsec

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	Jyaml Project	Jyaml	All	All	All	All
cpe:2.3:a:jyaml_project:jyaml:*.***.*.*.*.*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→