



CVE-2020-9493

Published on: 06/16/2021 12:00:00 AM UTC

Last Modified on: 04/08/2022 01:33:00 PM UTC

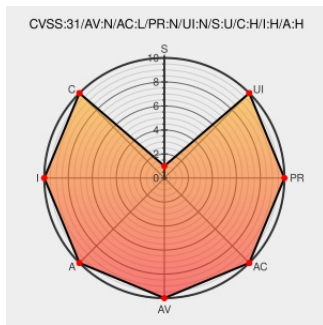
CVE-2020-9493

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Chainsaw](#) from [Apache](#) contain the following vulnerability:

A deserialization flaw was found in Apache Chainsaw versions prior to 2.1.0 which could lead to malicious code execution.

CVE-2020-9493 has been assigned by security@apache.org to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Apache Software Foundation](#) - [Apache Chainsaw](#) version < 2.1.0

Vulnerability Patch/Work Around

Don't configure Chainsaw to read serialized log events. Use a different receiver, such as XMLSocketReceiver

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: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
oss-security - CVE-2020-9493: Apache Chainsaw: Java deserialization in Chainsaw	www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2021/06/16/1
Pony Mail!	lists.apache.org text/html	MLIST [announce] 20210615 CVE-2020-9493: Apache Chainsaw: Java deserialization in Chainsaw
oss-security - CVE-2020-9493: Apache Chainsaw: Java deserialization in Chainsaw	www.openwall.com text/html	MLIST [oss-security] 20210615 CVE-2020-9493: Apache Chainsaw: Java deserialization in Chainsaw
oss-security - CVE-2022-23307: Apache Log4j 1.x: A deserialization flaw in the Chainsaw component of Log4j 1 can lead to malicious code execution.	www.openwall.com text/html	MLIST [oss-security] 20220118 CVE-2022-23307: Apache Log4j 1.x: A deserialization flaw in the Chainsaw component of Log4j 1 can lead to malicious code execution.

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.

Related QID Numbers

[730542](#) Atlassian Confluence Server and Confluence Data Center Log4j Multiple Vulnerabilities (CONFSERVER-78991)

[730566](#) Atlassian Jira Server and Data Center Log4j Vulnerability (JRASERVER-73885)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Chainsaw	All	All	All	All
Application	Apache	Log4j	All	All	All	All
Application	Qos	Reload4j	All	All	All	All
cpe:2.3:a:apache:chainsaw:*:*:*:*:*:						
cpe:2.3:a:apache:log4j:*:*:*:*:*:						
cpe:2.3:a:qos:reload4j:*:*:*:*:*:						

Discovery Credit

This issue was reported by [@kingkk](#)

Social Mentions

Source	Title	Posted (UTC)
@oss_security	CVE-2020-9493: Apache Chainsaw: Java deserialization in Chainsaw: Posted by Robert Middleton on Jun 15Reply-to: gen... twitter.com/i/web/status/1...	2021-06-16 05:03:02
@CVEreport	CVE-2020-9493 : A deserialization flaw was found in #Apache Chainsaw versions prior to 2.1.0 which could lead to ma... twitter.com/i/web/status/1...	2021-06-16 07:36:06
/r/netcve	CVE-2020-9493	2021-06-16 08:41:22

© [CVE.report](#) 2023 [🐦](#) [N](#) |

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](#)