



# CVE-2021-3100

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-3100
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@paloaltonetworks.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-19 23:15:00 UTC
<b>Updated</b>	2022-10-06 16:08:00 UTC
<b>Description</b>	The Apache Log4j hotpatch package before log4j-cve-2021-44228-hotpatch-1.1-13 didn't mimic the permissions of the JVM

## Risk And Classification

**Problem Types:** CWE-269

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Amazon</a>	<a href="#">Log4jhotpatch</a>	All	All	All	All
Application	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All

## References

Reference	Source	Link	Tags
ALAS2-2021-1732	MISC	<a href="#">alas.aws.amazon.com</a>	
AWS's Log4Shell Hot Patch Vulnerable to Container Escape and Privilege Escalation	MISC	<a href="#">unit42.paloaltonetworks.com</a>	
ALAS-2021-1554	MISC	<a href="#">alas.aws.amazon.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Yuval Avrahami, Palo Alto Networks

There are currently no legacy QID mappings associated with this CVE.

---

© [CVE.report](#) 2026 |

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](#)**