



CVE-2021-42697

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

Summary

CVE	CVE-2021-42697
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-02 22:15:00 UTC
Updated	2022-06-13 15:41:00 UTC
Description	Akka HTTP 10.1.x before 10.1.15 and 10.2.x before 10.2.7 can encounter stack exhaustion while parsing HTTP headers, w

Risk And Classification

Problem Types: CWE-674

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Akka	Http Server	All	All	All	All

References

Reference	Source	Link
Akka HTTP 10.1.14 Denial Of Service ≈ Packet Storm	MISC	packetstormse
News & Articles Akka	MISC	akka.io
CVE-2021-42697: Stack overflow while parsing User-Agent header with deeply nested comments • Akka HTTP	MISC	doc.akka.io
Akka HTTP 10.2.7 Released Akka	MISC	akka.io
Akka HTTP 10.1.15 Released Akka	MISC	akka.io
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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](#)