



CVE-2021-23339

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

Summary

CVE	CVE-2021-23339
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-17 08:15:00 UTC
Updated	2021-03-11 16:33:00 UTC
Description	This affects all versions before 10.1.14 and from 10.2.0 to 10.2.4 of package com.typesafe.akka:akka-http-core. It allows m

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lightbend	Akka-http	All	All	All	All
Application	Lightbend	Akka-http	All	All	All	All

References

Reference	Source
HTTP Request Smuggling in com.typesafe.akka:akka-http-core Snyk	MISC
github.com/akka/akka-http/pull/3754%23issuecomment-779265201	MISC
core: disallow parsing of Transfer-Encoding other than chunked by johanandren · Pull Request #3754 · akka/akka-http · GitHub	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: jrudolph

Legacy QID Mappings

[982633](#) Java (maven) Security Update for com.typesafe.akka:akka-http-core (GHSA-2w7w-2i92-44hx)

© [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](#)