



Netty: HTTP Request Smuggling via Chunked Extension Quoted-String Parsing

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

Summary

CVE	CVE-2026-33870
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 20:16:34 UTC
Updated	2026-03-30 20:12:16 UTC
Description	Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.132.Final and 4.2.10.Final, N

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security-advisories@github.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Problem Types: CWE-444 | CWE-444 CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netty	Netty	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Netty	Netty	affected < 4.1.132.Final	Not specified
CNA	Netty	Netty	affected >= 4.2.0.Alpha1, < 4.2.10.Final	Not specified

References

Reference	Source	Link	Tags
w4ke.info/2025/10/29/funky-chunks-2.html	security-advisories@github.com	w4ke.info	Technical Descrip
github.com/netty/netty/security/advisories/GHSA-pwqr-wmgm-9rr8	security-advisories@github.com	github.com	Exploit, Mitigation
w4ke.info/2025/06/18/funky-chunks.html	security-advisories@github.com	w4ke.info	Technical Descrip
www.rfc-editor.org/rfc/rfc9110	security-advisories@github.com	www.rfc-editor.org	Technical Descrip
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

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