



CVE-2019-16869

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

Summary

CVE	CVE-2019-16869
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-26 16:15:00 UTC
Updated	2023-11-07 03:06:00 UTC
Description	Netty before 4.1.42.Final mishandles whitespace before the colon in HTTP headers (such as a "Transfer-Encoding : chunke

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Netty	Netty	All	All	All	All
Application	Netty	Netty	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.2	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.3	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.4	All	All	All

References

Reference

Pony Mail!

Red Hat Customer Portal

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[cassandra-commits] 20210924 [jira] [Updated] (CASSANDRA-15417) CVE-2019-16869(Netty is vulnerable to HTTP Request Smuggling) of s

Pony Mail!

Bugtraq: [SECURITY] [DSA 4597-1] netty security update

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Debian -- Security Information -- DSA-4597-1 netty

Pony Mail!

[SECURITY] [DLA 1941-1] netty security update

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[SECURITY] [DLA 2365-1] netty-3.9 security update

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
[SECURITY] [DLA 2110-1] netty-3.9 security update
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
http request smuggling, cause by obfuscating TE header · Issue #9571 · netty/netty · GitHub
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[cassandra-commits] 20210924 [jira] [Commented] (CASSANDRA-15417) CVE-2019-16869(Netty is vulnerable to HTTP Request Smuggling)

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Comparing netty-4.1.41.Final...netty-4.1.42.Final · netty/netty · GitHub

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

USN-4532-1: Netty vulnerabilities | Ubuntu security notices | Ubuntu

Red Hat Customer Portal

Pony Mail!

Pony Mail!

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980656 Java (maven) Security Update for io.netty:netty-all (GHSA-p979-4mfw-53vg)

© [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](#)