



tls: make sure to abort the stream if headers are bogus

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

Summary

CVE	CVE-2025-39946
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-04 08:15:47 UTC
Updated	2026-04-02 09:16:19 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: tls: make sure to abort the stream if headers are bogus Nc

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 84c61fe1a75b4255df1e1e7c054c9e6d048da417 b36462146d86b1f22e594fe4dae611dffacfb203 git
CNA	Linux	Linux	affected 84c61fe1a75b4255df1e1e7c054c9e6d048da417 4cefe5be73886f383639fe0850bb72d5b568a7b9 git
CNA	Linux	Linux	affected 84c61fe1a75b4255df1e1e7c054c9e6d048da417 208640e6225cc929a05adbf79d1df558add3e231 git
CNA	Linux	Linux	affected 84c61fe1a75b4255df1e1e7c054c9e6d048da417 61ca2da5fb8f433ce8bbd1657c84a86272133e6b git
CNA	Linux	Linux	affected 84c61fe1a75b4255df1e1e7c054c9e6d048da417 0aeb54ac4cd5cf8f60131b4d9ec0b6dc9c27b20d git
CNA	Linux	Linux	affected 6.0
CNA	Linux	Linux	unaffected 6.0 semver
CNA	Linux	Linux	unaffected 6.1.154 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.108 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.49 6.12.* semver
CNA	Linux	Linux	unaffected 6.16.9 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/61ca2da5fb8f433ce8bbd1657c84a86272133e6b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/4cefe5be73886f383639fe0850bb72d5b568a7b9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/208640e6225cc929a05adbf79d1df558add3e231	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/b36462146d86b1f22e594fe4dae611dffacfb203	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/0aeb54ac4cd5cf8f60131b4d9ec0b6dc9c27b20d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](#)