net/tcp-md5: Fix MAC comparison to be constant-time

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-43383
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:49 UTC
Updated	2026-05-11 08:16:12 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net/tcp-md5: Fix MAC comparison to be constant-time To

Risk And Classification

Primary CVSS: v3.1 9.4 CRITICAL from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000240000 probability, percentile 0.070400000 (date 2026-05-10)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	9.4	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H
3.1	CNA	DECLARED	9.4	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected cfb6eeb4c860592edd123fdea908d23c6ad1c7dc 821c8751fdeecdeecabeb11704dd33439c9e4bbc git
CNA	Linux	Linux	affected cfb6eeb4c860592edd123fdea908d23c6ad1c7dc 345a9530756528d7ca407663d659c3c40e75c3dd gi
CNA	Linux	Linux	affected cfb6eeb4c860592edd123fdea908d23c6ad1c7dc 5d305a95130a8d08b9545e47f1e18d29d59866cb git
CNA	Linux	Linux	affected cfb6eeb4c860592edd123fdea908d23c6ad1c7dc 02669e2a4d207068edce7e8b5fafd85822018ce6 git
CNA	Linux	Linux	affected cfb6eeb4c860592edd123fdea908d23c6ad1c7dc ae3831b44f477de048287493e184fc3ff913b624 git
CNA	Linux	Linux	affected cfb6eeb4c860592edd123fdea908d23c6ad1c7dc b502e97e29d791ff7a8051f29a414535739be218 git
CNA	Linux	Linux	affected cfb6eeb4c860592edd123fdea908d23c6ad1c7dc 46d0d6f50dab706637f4c18a470aac20a21900d3 git
CNA	Linux	Linux	affected 2.6.20
CNA	Linux	Linux	unaffected 2.6.20 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.19 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.9 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/821c8751fdeecdeecabeb11704dd33439c9e4bbc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b502e97e29d791ff7a8051f29a414535739be218	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/5d305a95130a8d08b9545e47f1e18d29d59866cb	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/46d0d6f50dab706637f4c18a470aac20a21900d3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ae3831b44f477de048287493e184fc3ff913b624	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/02669e2a4d207068edce7e8b5fafd85822018ce6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/345a9530756528d7ca407663d659c3c40e75c3dd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**