tls: Fix race condition in tls_sw_cancel_work_tx()

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

Summary

CVE	CVE-2026-23240
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-10 18:18:13 UTC
Updated	2026-04-02 15:16:25 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: tls: Fix race condition in tls_sw_cancel_work_tx() This issu

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000570000 probability, percentile 0.179130000 (date 2026-04-07)

Version	Source	Type	Score	Severity	Vector
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

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected f87e62d45e51b12d48d2cb46b5cde8f83b866bc4 a5de36d6cee74a92c1a21b260bc507e64bc451de gi
CNA	Linux	Linux	affected f87e62d45e51b12d48d2cb46b5cde8f83b866bc4 854cd32bc74fe573353095e90958490e4e4d641b gi
CNA	Linux	Linux	affected f87e62d45e51b12d48d2cb46b5cde8f83b866bc4 17153f154f80be2b47ebf52840f2d8f724eb2f3b git
CNA	Linux	Linux	affected f87e62d45e51b12d48d2cb46b5cde8f83b866bc4 7bb09315f93dce6acc54bf59e5a95ba7365c2be4 git
CNA	Linux	Linux	affected 5.3
CNA	Linux	Linux	unaffected 5.3 semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0-rc2 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/17153f154f80be2b47ebf52840f2d8f724eb2f3b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a5de36d6cee74a92c1a21b260bc507e64bc451de	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/854cd32bc74fe573353095e90958490e4e4d641b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/7bb09315f93dce6acc54bf59e5a95ba7365c2be4	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**