net/tls: fix use-after-free in -EBUSY error path of tls_do_encryption

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

Summary

CVE	CVE-2026-31533
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 18:16:26 UTC
Updated	2026-04-24 14:38:44 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net/tls: fix use-after-free in -EBUSY error path of tls_do_er

Risk And Classification

EPSS: 0.000140000 probability, percentile 0.026590000 (date 2026-04-24)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 3ade391adc584f17b5570fd205de3ad029090368 414fc5e5a5aff776c150f1b86770e0a25a35df3a git
CNA	Linux	Linux	affected cd1bbca03f3c1d845ce274c0d0a66de8e5929f72 02f3ecadb23558bbe068e6504118f1b712d4ece0 git
CNA	Linux	Linux	affected 13eca403876bbea3716e82cdfe6f1e6febb38754 0e43e0a3c94044acc74b8e0927c27972eb5a59e8 git
CNA	Linux	Linux	affected 8590541473188741055d27b955db0777569438e3 aa9facde6c5005205874c37db3fd25799d741baf gi
CNA	Linux	Linux	affected 8590541473188741055d27b955db0777569438e3 5d70eb25b41e9b010828cd12818b06a0c3b04412
CNA	Linux	Linux	affected 8590541473188741055d27b955db0777569438e3 2694d408b0e595024e0fc1d64ff9db0358580f74 git
CNA	Linux	Linux	affected 8590541473188741055d27b955db0777569438e3 a9b8b18364fffce4c451e6f6fd218fa4ab646705 git
CNA	Linux	Linux	affected ab6397f072e5097f267abf5cb08a8004e6b17694 git
CNA	Linux	Linux	affected 6.8
CNA	Linux	Linux	unaffected 6.8 semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.169 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.135 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.82 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.23 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.13 6.19.* semver

CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/02f3ecadb23558bbe068e6504118f1b712d4ece0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/414fc5e5a5aff776c150f1b86770e0a25a35df3a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/5d70eb25b41e9b010828cd12818b06a0c3b04412	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2694d408b0e595024e0fc1d64ff9db0358580f74	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/0e43e0a3c94044acc74b8e0927c27972eb5a59e8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a9b8b18364fffce4c451e6f6fd218fa4ab646705	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/aa9facde6c5005205874c37db3fd25799d741baf	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.