



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

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

## Summary

<b>CVE</b>	CVE-2026-31533
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-23 18:16:26 UTC
<b>Updated</b>	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_en`

## Risk And Classification

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

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3ade391adc584f17b5570fd205de3ad029090368 414fc5e5a5aff776c150f1b86770e0a25a35df3a git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected cd1bbca03f3c1d845ce274c0d0a66de8e5929f72 02f3ecadb23558bbe068e6504118f1b712d4ece0 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 13eca403876bbea3716e82cdf6f1e6febb38754 0e43e0a3c94044acc74b8e0927c27972eb5a59e8 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8590541473188741055d27b955db0777569438e3 aa9facde6c5005205874c37db3fd25799d741baf gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8590541473188741055d27b955db0777569438e3 5d70eb25b41e9b010828cd12818b06a0c3b04412
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8590541473188741055d27b955db0777569438e3 2694d408b0e595024e0fc1d64ff9db0358580f74 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8590541473188741055d27b955db0777569438e3 a9b8b18364ffce4c451e6f6fd218fa4ab646705 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ab6397f072e5097f267abf5cb08a8004e6b17694 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.8
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.8 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15.203 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.169 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.135 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.82 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.23 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.13 6.19.* semver

## References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/02f3ecadb23558bbe068e6504118f1b712d4ece0">git.kernel.org/stable/c/02f3ecadb23558bbe068e6504118f1b712d4ece0</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/414fc5e5a5aff776c150f1b86770e0a25a35df3a">git.kernel.org/stable/c/414fc5e5a5aff776c150f1b86770e0a25a35df3a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/5d70eb25b41e9b010828cd12818b06a0c3b04412">git.kernel.org/stable/c/5d70eb25b41e9b010828cd12818b06a0c3b04412</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/2694d408b0e595024e0fc1d64ff9db0358580f74">git.kernel.org/stable/c/2694d408b0e595024e0fc1d64ff9db0358580f74</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/0e43e0a3c94044acc74b8e0927c27972eb5a59e8">git.kernel.org/stable/c/0e43e0a3c94044acc74b8e0927c27972eb5a59e8</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/a9b8b18364ffce4c451e6f6fd218fa4ab646705">git.kernel.org/stable/c/a9b8b18364ffce4c451e6f6fd218fa4ab646705</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/aa9facde6c5005205874c37db3fd25799d741baf">git.kernel.org/stable/c/aa9facde6c5005205874c37db3fd25799d741baf</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)