



usb: gadget: f_rndis: Protect RNDIS options with mutex

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-43342
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 14:16:44 UTC
Updated	2026-05-08 14:16:44 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_rndis: Protect RNDIS options with mutex TI

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 73517cf49bd449122b615d2b7a6bb835f02252e5 0a75d97c53477a59c0aa1c65f69038c719f9c5b8 git
CNA	Linux	Linux	affected 73517cf49bd449122b615d2b7a6bb835f02252e5 c1b3d5b0acb194efe20fc5864ee03439fa7bd45c git
CNA	Linux	Linux	affected 73517cf49bd449122b615d2b7a6bb835f02252e5 65b7dbf80a1627667c241fff7c1c224f3118014f git
CNA	Linux	Linux	affected 73517cf49bd449122b615d2b7a6bb835f02252e5 cb5316b37288ab8791584e32f114c4f41ad45b67 git
CNA	Linux	Linux	affected 73517cf49bd449122b615d2b7a6bb835f02252e5 7d8fa3b8783ab95a46e20d97fbeeede719b2efda git
CNA	Linux	Linux	affected 73517cf49bd449122b615d2b7a6bb835f02252e5 446f1842cda929c40d4697722bfdcfb334bc9692 git
CNA	Linux	Linux	affected 73517cf49bd449122b615d2b7a6bb835f02252e5 209decd3f7901df9842b83f2540dc8685e344a07 git
CNA	Linux	Linux	affected 73517cf49bd449122b615d2b7a6bb835f02252e5 8d8c68b1fc06ece60cf43e1306ff0f4ac121547e git
CNA	Linux	Linux	affected 4.14
CNA	Linux	Linux	unaffected 4.14 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.134 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.81 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.22 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.12 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/209decd3f7901df9842b83f2540dc8685e344a07	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/65b7dbf80a1627667c241fff7c1c224f3118014f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8d8c68b1fc06ece60cf43e1306ff0f4ac121547e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/0a75d97c53477a59c0aa1c65f69038c719f9c5b8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/cb5316b37288ab8791584e32f114c4f41ad45b67	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/7d8fa3b8783ab95a46e20d97fbeeede719b2efda	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c1b3d5b0acb194efe20fc5864ee03439fa7bd45c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/446f1842cda929c40d4697722bfdcfb334bc9692	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
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](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](#).

Free CVE JSON API cve.report/api

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