bridge: br_nd_send: linearize skb before parsing ND options

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

Summary

CVE	CVE-2026-31682
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-25 09:16:01 UTC
Updated	2026-04-25 09:16:01 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: bridge: br_nd_send: linearize skb before parsing ND optio

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected ed842faeb2bd49256f00485402f3113205f91d30 c68433fd291c9e88c00292095172c62d1997d662 git
CNA	Linux	Linux	affected ed842faeb2bd49256f00485402f3113205f91d30 4f397b950c916e9a1f8a4fce04ea0110206cad47 git
CNA	Linux	Linux	affected ed842faeb2bd49256f00485402f3113205f91d30 bd91ec85aa4c77d645bd2739fc56784157a88ca2 git
CNA	Linux	Linux	affected ed842faeb2bd49256f00485402f3113205f91d30 658261898130da620fc3d0fbb0523efb3366cb55 git
CNA	Linux	Linux	affected ed842faeb2bd49256f00485402f3113205f91d30 2ba4caba423ed94d63006eb1d2227b0332ab7fcd git
CNA	Linux	Linux	affected ed842faeb2bd49256f00485402f3113205f91d30 9c55e41c73af5c4511070933b1bd25248521270c git
CNA	Linux	Linux	affected ed842faeb2bd49256f00485402f3113205f91d30 3a30f6469b058574f49efde61cd6f5d79e576053 git
CNA	Linux	Linux	affected ed842faeb2bd49256f00485402f3113205f91d30 a01aee7cafc575bb82f5529e8734e7052f9b16ea git
CNA	Linux	Linux	affected 4.15
CNA	Linux	Linux	unaffected 4.15 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/658261898130da620fc3d0fbb0523efb3366cb55	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/3a30f6469b058574f49efde61cd6f5d79e576053	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a01aee7cafc575bb82f5529e8734e7052f9b16ea	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c68433fd291c9e88c00292095172c62d1997d662	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9c55e41c73af5c4511070933b1bd25248521270c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2ba4caba423ed94d63006eb1d2227b0332ab7fcd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/4f397b950c916e9a1f8a4fce04ea0110206cad47	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/bd91ec85aa4c77d645bd2739fc56784157a88ca2	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.