bonding: prevent potential infinite loop in bond_header_parse()

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

Summary

CVE	CVE-2026-23451
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-03 16:16:31 UTC
Updated	2026-04-07 13:21:09 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: bonding: prevent potential infinite loop in bond_header_pa

Risk And Classification

EPSS: 0.000180000 probability, percentile 0.044120000 (date 2026-04-06)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 9baf26a91565b7bb2b1d9f99aaf884a2b28c2f6d 946bb6cacf0ccada7bc80f1cfa07c1ed79511c1c git
CNA	Linux	Linux	affected 6ac890f1d60ac3707ee8dae15a67d9a833e49956 4172a7901cf43fe1cc63ef7a2ef33735ff7b7d13 git
CNA	Linux	Linux	affected 95597d11dc8bddb2b9a051c9232000bfbb5e43ba 9b49c854f14f5e2d493e562a1e28d2e57fe37371 git
CNA	Linux	Linux	affected 950803f7254721c1c15858fbbfae3deaaeeecb11 b7405dcf7385445e10821777143f18c3ce20fa04 git
CNA	Linux	Linux	affected 7.0-rc4
CNA	Linux	Linux	unaffected 7.0-rc4 semver
CNA	Linux	Linux	unaffected 6.18.20 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.10 6.19.* semver
CNA	Linux	Linux	unaffected 7.0-rc5 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/b7405dcf7385445e10821777143f18c3ce20fa04	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/4172a7901cf43fe1cc63ef7a2ef33735ff7b7d13	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9b49c854f14f5e2d493e562a1e28d2e57fe37371	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/946bb6cacf0ccada7bc80f1cfa07c1ed79511c1c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	

CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.