geneve: Fix use-after-free in geneve_find_dev().

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

Summary

CVE	CVE-2025-21858
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-03-12 10:15:18 UTC
Updated	2026-05-12 13:16:38 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: geneve: Fix use-after-free in geneve_find_dev(). syzkaller

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-416 | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 2d07dc79fe04a43d82a346ced6bbf07bdb523f1b d5e86e
CNA	Linux	Linux	affected 2d07dc79fe04a43d82a346ced6bbf07bdb523f1b 5a0538
CNA	Linux	Linux	affected 2d07dc79fe04a43d82a346ced6bbf07bdb523f1b f74f656
CNA	Linux	Linux	affected 2d07dc79fe04a43d82a346ced6bbf07bdb523f1b 904e74
CNA	Linux	Linux	affected 2d07dc79fe04a43d82a346ced6bbf07bdb523f1b 3ce92c
CNA	Linux	Linux	affected 2d07dc79fe04a43d82a346ced6bbf07bdb523f1b da9b0a
CNA	Linux	Linux	affected 2d07dc79fe04a43d82a346ced6bbf07bdb523f1b 788dbc
CNA	Linux	Linux	affected 2d07dc79fe04a43d82a346ced6bbf07bdb523f1b 959317
CNA	Linux	Linux	affected 4.2
CNA	Linux	Linux	unaffected 4.2 semver
CNA	Linux	Linux	unaffected 5.4.291 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.235 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.179 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.130 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.80 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.17 6.12.* semver
CNA	Linux	Linux	unaffected 6.13.5 6.13.* semver
CNA	Linux	Linux	unaffected 6.14 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
git.kernel.org/stable/c/f74f6560146714241c6e167b03165ee77a86e316	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/05/msg00030.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/3ce92ca990cfac88a87c61df3cc0b5880e688ecf	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

git.kernel.org/stable/c/9593172d93b9f91c362baec4643003dc29802929	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/5a0538ac6826807d6919f6aecbb8996c2865af2c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/788dbca056a8783ec063da3c9d49a3a71c76c283	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/da9b0ae47f084014b1e4b3f31f70a0defd047ff3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/904e746b2e7fa952ab8801b303ce826a63153d78	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/d5e86e27de0936f3cb0a299ce519d993e9cf3886	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/05/msg00045.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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