net/smc: fix one NULL pointer dereference in smc_ib_is_sg_need_sync()

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

Summary

CVE	CVE-2025-39857
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-19 16:15:44 UTC
Updated	2026-05-12 13:17:16 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix one NULL pointer dereference in smc_ib_is_s

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-476

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/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 0ef69e788411cba2af017db731a9fc62d255e9ac 0cdf1fd8fc59d44a48c6943246111369103
CNA	Linux	Linux	affected 0ef69e788411cba2af017db731a9fc62d255e9ac f18d9b3abf9c6587372cc702f963a759227
CNA	Linux	Linux	affected 0ef69e788411cba2af017db731a9fc62d255e9ac eb929910bd4b4165920fa06a87b22cc6ca
CNA	Linux	Linux	affected 0ef69e788411cba2af017db731a9fc62d255e9ac 34f17cbe027050b8d5316ea1b6f9bd7c37
CNA	Linux	Linux	affected 0ef69e788411cba2af017db731a9fc62d255e9ac ba1e9421cf1a8369d25c3832439702a015
CNA	Linux	Linux	affected 6.0
CNA	Linux	Linux	unaffected 6.0 semver
CNA	Linux	Linux	unaffected 6.1.151 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.105 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.46 6.12.* semver
CNA	Linux	Linux	unaffected 6.16.6 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

References

Reference	Source	Link
git.kernel.org/stable/c/eb929910bd4b4165920fa06a87b22cc6cae92e0e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/ba1e9421cf1a8369d25c3832439702a015d6b5f9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/34f17cbe027050b8d5316ea1b6f9bd7c378e92de	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/f18d9b3abf9c6587372cc702f963a7592277ed56	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/0cdf1fd8fc59d44a48c694324611136910301ef9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.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.