Bluetooth: Fix use-after-free in l2cap_sock_cleanup_listen()

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

Summary

CVE	CVE-2025-39860
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: Bluetooth: Fix use-after-free in l2cap_sock_cleanup_listen

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

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 a2da00d1ea1abfb04f846638e210b5b5166e3
CNA	Linux	Linux	affected 06f87c96216bc5cd1094c23492274f77f1d5d
CNA	Linux	Linux	affected fbe5a2fed8156cc19eb3b956602b0a1dd46a3
CNA	Linux	Linux	affected 29fac18499332211b2615ade356e2bd8b326
CNA	Linux	Linux	affected 1728137b33c00d5a2b5110ed7aafb42e7c32
CNA	Linux	Linux	affected 1728137b33c00d5a2b5110ed7aafb42e7c32
CNA	Linux	Linux	affected 1728137b33c00d5a2b5110ed7aafb42e7c32
CNA	Linux	Linux	affected 1728137b33c00d5a2b5110ed7aafb42e7c32
CNA	Linux	Linux	affected 51822644a047eac2310fab0799b64e3430b5
CNA	Linux	Linux	affected 82cdb2ccbe43337798393369f0ceb98699fe6
CNA	Linux	Linux	affected 10426afe65c8bf7b24dd0c7be4dcc65f86fc99
CNA	Linux	Linux	affected 6.5
CNA	Linux	Linux	unaffected 6.5 semver
CNA	Linux	Linux	unaffected 5.4.299 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.243 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.192 5.15.* 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	RUGGEDCOM RST2428P	affected V3.3 custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	affected V3.3 custom
ADP	Siemens	SCALANCE XCH328	affected V3.3 custom
ADP	Siemens	SCALANCE XCM324	affected V3.3 custom
ADP	Siemens	SCALANCE XCM328	affected V3.3 custom
ADP	Siemens	SCALANCE XCM332	affected V3.3 custom
ADP	Siemens	SCALANCE XRH334 24 V DC 8xFO CC	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 230 V AC 12xFO	affected V3.3 custom

ADP	Siemens	SCALANCE XRM334 230 V AC 8xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 230V AC 2x10G 24xSFP 8xSFP	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 24 V DC 12xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 24 V DC 8xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 24V DC 2x10G 24xSFP 8xSFP	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 2x230 V AC 12xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 2x230 V AC 8xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 2x230V AC 2x10G 24xSFP 8xSFP	affected V3.3 custom
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

References

Reference	Source	Link
git.kernel.org/stable/c/83e1d9892ef51785cf0760b7681436760dda435a	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/47f6090bcf75c369695d21c3f179db8a56bbbd49	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/964cbb198f9c46c2b2358cd1faffc04c1e8248cf	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-089022.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/862c628108562d8c7a516a900034823b381d3cba	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/6077d16b5c0f65d571eee709de2f0541fb5ef0ca	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.cc
git.kernel.org/stable/c/3dff390f55ccd9ce12e91233849769b5312180c2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/2ca99fc3512a8074de20ee52a87b492dfcc41a4d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/306b0991413b482dbf5585b423022123bb505966	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00007.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.

Free CVE JSON API cve.report/api

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