sctp: sysctl: rto_min/max: avoid using current->nsproxy

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

Summary

CVE	CVE-2025-21639
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-01-19 11:15:09 UTC
Updated	2026-05-12 13:16:30 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: sctp: sysctl: rto_min/max: avoid using current->nsproxy As

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 | CWE-476 CWE-476 NULL Pointer Dereference

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

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 4f3fdf3bc59cafd14c3bc2c2369efad34c7aa8b5 c8d179f3
CNA	Linux	Linux	affected 4f3fdf3bc59cafd14c3bc2c2369efad34c7aa8b5 246428bf
CNA	Linux	Linux	affected 4f3fdf3bc59cafd14c3bc2c2369efad34c7aa8b5 0f78f094
CNA	Linux	Linux	affected 4f3fdf3bc59cafd14c3bc2c2369efad34c7aa8b5 4059507
CNA	Linux	Linux	affected 4f3fdf3bc59cafd14c3bc2c2369efad34c7aa8b5 dc9d0e3
CNA	Linux	Linux	affected 4f3fdf3bc59cafd14c3bc2c2369efad34c7aa8b5 c87f1f6a
CNA	Linux	Linux	affected 4f3fdf3bc59cafd14c3bc2c2369efad34c7aa8b5 9fc17b76
CNA	Linux	Linux	affected 3.13
CNA	Linux	Linux	unaffected 3.13 semver
CNA	Linux	Linux	unaffected 5.4.290 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.234 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.177 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.125 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.72 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.10 6.12.* semver
CNA	Linux	Linux	unaffected 6.13 * 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/246428bfb9e7db15c5cd08e1d0eca41b65af2b06	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/03/msg00002.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/dc9d0e3cfd16f66fbf0862857c6b391c8613ca9f	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/0f78f09466744589e420935e646ae78212a38290	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

git.kernel.org/stable/c/c87f1f6ade56c711f8736901e330685b453e420e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/9fc17b76fc70763780aa78b38fcf4742384044a5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/c8d179f3b1c1d60bf4484f50aa67b4c70f91bff9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/03/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/4059507e34aa5fe0fa9fd5b2b5f0c8b26ab2d482	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.