tcp: drop secpath at the same time as we currently drop dst

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

Summary

CVE	CVE-2025-21864
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-03-12 10:15:19 UTC
Updated	2026-05-12 13:16:39 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: tcp: drop secpath at the same time as we currently drop ds

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

ntegrity

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 68822bdf76f10c3dc80609d4e2cdc1e847429086 87858bbf21d
CNA	Linux	Linux	affected 68822bdf76f10c3dc80609d4e2cdc1e847429086 f1d5e6a5e46
CNA	Linux	Linux	affected 68822bdf76f10c3dc80609d4e2cdc1e847429086 cd34a07f744
CNA	Linux	Linux	affected 68822bdf76f10c3dc80609d4e2cdc1e847429086 69cafd94130
CNA	Linux	Linux	affected 68822bdf76f10c3dc80609d4e2cdc1e847429086 9b6412e6979
CNA	Linux	Linux	affected 5.19
CNA	Linux	Linux	unaffected 5.19 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 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom

References

Reference	Source	Link
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/f1d5e6a5e468308af7759cf5276779d3155c5e98	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/69cafd9413084cd5012cf5d7c7ec6f3d493726d9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/9b6412e6979f6f9e0632075f8f008937b5cd4efd	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
git.kernel.org/stable/c/87858bbf21da239ace300d61dd209907995c0491	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/cd34a07f744451e2ecf9005bb7d24d0b2fb83656	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.