



net: avoid potential underflow in qdisc_pkt_len_init() with UFO

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2024-49949
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-21 18:15:16 UTC
Updated	2026-05-12 12:17:18 UTC

Description In the Linux kernel, the following vulnerability has been resolved: net: avoid potential underflow in qdisc_pkt_len_init() with l

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 960b360ca7463921c1a6b72e7066a706d640			
CNA	Linux	Linux	affected fb2dbc124a7f800cd0e4f901a1bbb769a0171			
CNA	Linux	Linux	affected 8e6bae950da9dc2d2c6c18b1c6b206dc00dc			
CNA	Linux	Linux	affected 0f810d06b507aa40fef8d1ac0a88e6d0590db			
CNA	Linux	Linux	affected cf9acc90c80ecbee00334aa85d92f4e74014b			
CNA	Linux	Linux	affected cf9acc90c80ecbee00334aa85d92f4e74014b			
CNA	Linux	Linux	affected cf9acc90c80ecbee00334aa85d92f4e74014b			
CNA	Linux	Linux	affected cf9acc90c80ecbee00334aa85d92f4e74014b			
CNA	Linux	Linux	affected cf9acc90c80ecbee00334aa85d92f4e74014b			
CNA	Linux	Linux	affected 2128303bff700c857739a0af8cc39c1a41840			
CNA	Linux	Linux	affected 5.16			
CNA	Linux	Linux	unaffected 5.16 semver			
CNA	Linux	Linux	unaffected 4.19.323 4.19.* semver			
CNA	Linux	Linux	unaffected 5.4.285 5.4.* semver			
CNA	Linux	Linux	unaffected 5.10.227 5.10.* semver			
CNA	Linux	Linux	unaffected 5.15.168 5.15.* semver			
CNA	Linux	Linux	unaffected 6.1.113 6.1.* semver			
CNA	Linux	Linux	unaffected 6.6.55 6.6.* semver			
CNA	Linux	Linux	unaffected 6.10.14 6.10.* semver			
CNA	Linux	Linux	unaffected 6.11.3 6.11.* semver			
CNA	Linux	Linux	unaffected 6.12 * original_commit_for_fix			
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.2 custom			
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	affected V3.2 custom			
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	affected V3.2 custom			
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom			
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom			
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom			
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom			
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom			

ADPSiemensSIPLUS S7-1500 CPU 1518-4 PN/DP MFPaffected V3.1.0 V3.1.5 custom

References

Reference	Source	Link
cert-portal.siemens.com/productcert/html/ssa-398330.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/d70ca7598943572d5e384227bd268acb5109bf72	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/d6114993e0a89fde84a60a60a8329a571580b174	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/f959cce8a2a04ce776aa8b78e83ce339e0d7fbac	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/939c88cbdc668dadd8cfa7a35d9066331239041c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/25ab0b87dbd89cecef8a9c60a02bb97832e471d1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/1598d70ad9c7d0a4d9d54b82094e9f45908fda6d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/81fd007dcd47c34471766249853e4d4bce8eea4b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/c20029db28399ecc50e556964eaba75c43b1e2f1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/ba26060a29d3ca1bfc737aa79f7125128f35147c	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.