ipv6: prevent possible NULL deref in fib6_nh_init()

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

Summary

CVE	CVE-2024-40961
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-07-12 13:15:18 UTC
Updated	2026-05-12 12:17:01 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent possible NULL deref in fib6_nh_init() syzbot

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 428604fb118facce1309670779a35baf27ad0
CNA	Linux	Linux	affected 428604fb118facce1309670779a35baf27ad0
CNA	Linux	Linux	affected 428604fb118facce1309670779a35baf27ad0
CNA	Linux	Linux	affected 428604fb118facce1309670779a35baf27ad0
CNA	Linux	Linux	affected 428604fb118facce1309670779a35baf27ad0
CNA	Linux	Linux	affected 428604fb118facce1309670779a35baf27ad0
CNA	Linux	Linux	affected 428604fb118facce1309670779a35baf27ad0
CNA	Linux	Linux	affected 4.17
CNA	Linux	Linux	unaffected 4.17 semver
CNA	Linux	Linux	unaffected 5.4.279 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.221 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.162 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.96 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.36 6.6.* semver
CNA	Linux	Linux	unaffected 6.9.7 6.9.* semver
CNA	Linux	Linux	unaffected 6.10 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 custom
ADP	Siemens	RUGGEDCOM RST2428P	unaffected * custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	affected V3.1 custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	unaffected * custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
git.kernel.org/stable/c/4cdfe813015d5a24586bd0a84fa0fa6eb0a1f668	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/88b9a55e2e35ea846d41f4efdc29d23345bd1aa4	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/2eab4543a2204092c3a7af81d7d6c506e59a03a6	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/ae8d3d39efe366c2198f530e01e4bf07830bf403	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org

cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/b6947723c9eabcab58cfb33cdb0a565a6aee6727	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/de5ad4d45cd0128a2a37555f48ab69aa19d78adc	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/3200ffeec4d59aad5bc9ca75d2c1fae47c0aeade	af854a3a-2127-422b-91ae-364da2661108	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.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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