ipv6: fix possible UAF in ip6_finish_output2()

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

Summary

CVE	CVE-2024-44986
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-09-04 20:15:07 UTC
Updated	2026-04-09 17:42:15 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible UAF in ip6_finish_output2() If skb_expan

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	Debian	Debian Linux	11.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 5796015fa968a3349027a27dcd04c71d95c53ba5 e891b36de161fcd96f12ff83667473e5067b9037 git
CNA	Linux	Linux	affected 5796015fa968a3349027a27dcd04c71d95c53ba5 3574d28caf9a09756ae87ad1ea096c6f47b6101e gi
CNA	Linux	Linux	affected 5796015fa968a3349027a27dcd04c71d95c53ba5 6ab6bf731354a6fdbaa617d1ec194960db61cf3b git
CNA	Linux	Linux	affected 5796015fa968a3349027a27dcd04c71d95c53ba5 56efc253196751ece1fc535a5b582be127b0578a gi
CNA	Linux	Linux	affected 5796015fa968a3349027a27dcd04c71d95c53ba5 da273b377ae0d9bd255281ed3c2adb228321687b g
CNA	Linux	Linux	affected ded37d03440d0ab346a8287cc2ba88b8dc90ceb0 git
CNA	Linux	Linux	affected 2323690eb05865a657709f4d28eb9538ea97bfc2 git
CNA	Linux	Linux	affected b34c668a867ffdcf8bd8db4a36512572e82b4a15 git
CNA	Linux	Linux	affected 5.14
CNA	Linux	Linux	unaffected 5.14 semver
CNA	Linux	Linux	unaffected 5.15.166 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.107 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.48 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.7 6.10.* semver
CNA	Linux	Linux	unaffected 6.11 * original_commit_for_fix

References

Reference	Source	Link	Tag
git.kernel.org/stable/c/da273b377ae0d9bd255281ed3c2adb228321687b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Pat
git.kernel.org/stable/c/6ab6bf731354a6fdbaa617d1ec194960db61cf3b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Pat
git.kernel.org/stable/c/56efc253196751ece1fc535a5b582be127b0578a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Pat
git.kernel.org/stable/c/e891b36de161fcd96f12ff83667473e5067b9037	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Pat
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Mai
git.kernel.org/stable/c/3574d28caf9a09756ae87ad1ea096c6f47b6101e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Pat
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

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**