ipv6: Fix use-after-free in inet6_addr_del().

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

Summary

CVE	CVE-2026-23010
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-25 15:15:55 UTC
Updated	2026-04-27 14:16:29 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix use-after-free in inet6_addr_del(). syzbot reporte

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected ca97dd10424860a3806ad3a9e26b9dce2901ee0c 6e89d60b4f03014f7d412ce64b17a840840d490e g
CNA	Linux	Linux	affected 836deb96383ed9c1a411f172954d74b3f74ec6ac 9356b69d03d0f50cce91cebdabd33dda023fbd64 git
CNA	Linux	Linux	affected cb74207ef98317f8874a0b9780bb339c2eb700b0 2684610a9c9c53f262fd864fa5c407e79f304804 git
CNA	Linux	Linux	affected 00b5b7aab9e422d00d5a9d03d7e0760a76b5d57f 8b6dcb565e419846bd521e31d5e1f98e4d0e1179 g
CNA	Linux	Linux	affected 00b5b7aab9e422d00d5a9d03d7e0760a76b5d57f ddf96c393a33aef4887e2e406c76c2f8cda1419c git
CNA	Linux	Linux	affected 851b3bb105c595cc20b8dcc1b4de029061ce2b76 git
CNA	Linux	Linux	affected 6.13
CNA	Linux	Linux	unaffected 6.13 semver
CNA	Linux	Linux	unaffected 6.1.162 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.122 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.67 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.7 6.18.* semver
CNA	Linux	Linux	unaffected 6.19 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/8b6dcb565e419846bd521e31d5e1f98e4d0e1179	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/ddf96c393a33aef4887e2e406c76c2f8cda1419c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/2684610a9c9c53f262fd864fa5c407e79f304804	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/6e89d60b4f03014f7d412ce64b17a840840d490e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/9356b69d03d0f50cce91cebdabd33dda023fbd64	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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**