



# net: ipv6: ndisc: fix ndisc\_ra\_useropt to initialize nduseropt\_padX fields to zero to prevent an info-leak

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-43040
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-01 15:16:50 UTC
<b>Updated</b>	2026-05-08 18:53:20 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: net: ipv6: ndisc: fix ndisc\_ra\_useropt to initialize nduserop

## Risk And Classification

**Primary CVSS:** v3.1 7.1 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

**EPSS:** 0.000240000 probability, percentile 0.068060000 (date 2026-05-05)

**Problem Types:** CWE-909

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/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 31910575a9de61e78065e93846e8e7a4894a18bf 1da9023f6b071a38e5430ffbce4b70b2b1ac4f9c git
CNA	Linux	Linux	affected 31910575a9de61e78065e93846e8e7a4894a18bf 2fe4d0ba690a69ad6ae9f7ab9bdc96e02610b648 g
CNA	Linux	Linux	affected 31910575a9de61e78065e93846e8e7a4894a18bf 11d7fe97421cfc81549940c20ed5ac9472d6db05 gi
CNA	Linux	Linux	affected 31910575a9de61e78065e93846e8e7a4894a18bf 7f56d87e527bb5a13c3e8b0d5840cb6332822f6d gi
CNA	Linux	Linux	affected 31910575a9de61e78065e93846e8e7a4894a18bf 4f810c686fde509d1cdaa706322d9d2531f8f1a4 git
CNA	Linux	Linux	affected 31910575a9de61e78065e93846e8e7a4894a18bf b485eef3d97b7aae55ce669b6de555ec81f3d21c gi
CNA	Linux	Linux	affected 31910575a9de61e78065e93846e8e7a4894a18bf ef3645606e4a635d5062a492f22b7f490852ee67 gi
CNA	Linux	Linux	affected 31910575a9de61e78065e93846e8e7a4894a18bf ae05340ccaa9d347fe85415609e075545bec589f gi
CNA	Linux	Linux	affected 2.6.24
CNA	Linux	Linux	unaffected 2.6.24 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.134 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.81 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.22 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.12 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/1da9023f6b071a38e5430ffbce4b70b2b1ac4f9c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/4f810c686fde509d1cdaa706322d9d2531f8f1a4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/ae05340ccaa9d347fe85415609e075545bec589f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/11d7fe97421cfc81549940c20ed5ac9472d6db05	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/7f56d87e527bb5a13c3e8b0d5840cb6332822f6d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/b485eef3d97b7aae55ce669b6de555ec81f3d21c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/ef3645606e4a635d5062a492f22b7f490852ee67	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch

git.kernel.org/stable/c/2fe4d0ba690a69ad6ae9f7ab9bdc96e02610b648	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonica

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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 registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)