



# netfilter: nf\_contrack\_h323: fix OOB read in decode\_int() CONS case

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

## Summary

<b>CVE</b>	CVE-2026-23456
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-03 16:16:32 UTC
<b>Updated</b>	2026-04-18 09:16:28 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: netfilter: nf\_contrack\_h323: fix OOB read in decode\_int()

## Risk And Classification

**EPSS:** 0.000320000 probability, percentile 0.090980000 (date 2026-04-18)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5e35941d990123f155b02d5663e51a24f816b6f3 a2cd54b9348e485d338b3c132338a4410c99afaf git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5e35941d990123f155b02d5663e51a24f816b6f3 c95dc674ebf01ecfb40388b6facfc89b81fed3b7 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5e35941d990123f155b02d5663e51a24f816b6f3 41b417ff73a24b2c68134992cc44c88db27f482d git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5e35941d990123f155b02d5663e51a24f816b6f3 52235bf88159a1ef16434ab49e47e99c8a09ab20 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5e35941d990123f155b02d5663e51a24f816b6f3 774a434f8c9c8602a976b2536f65d0172a07f4d2 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5e35941d990123f155b02d5663e51a24f816b6f3 6bce72daeccca9aa1746e92d6c3d4784e71f2ebb git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5e35941d990123f155b02d5663e51a24f816b6f3 fb6c3596823ec5dd09c2123340330d7448f51a59 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5e35941d990123f155b02d5663e51a24f816b6f3 1e3a3593162c96e8a8de48b1e14f60c3b57fca8a git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 2.6.17
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 2.6.17 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10.253 5.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15.203 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.167 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.130 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.78 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.20 6.18.* semver

CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.10 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/c95dc674ebf01ecfb40388b6facfc89b81fed3b7">git.kernel.org/stable/c/c95dc674ebf01ecfb40388b6facfc89b81fed3b7</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/fb6c3596823ec5dd09c2123340330d7448f51a59">git.kernel.org/stable/c/fb6c3596823ec5dd09c2123340330d7448f51a59</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/774a434f8c9c8602a976b2536f65d0172a07f4d2">git.kernel.org/stable/c/774a434f8c9c8602a976b2536f65d0172a07f4d2</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/52235bf88159a1ef16434ab49e47e99c8a09ab20">git.kernel.org/stable/c/52235bf88159a1ef16434ab49e47e99c8a09ab20</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/1e3a3593162c96e8a8de48b1e14f60c3b57fca8a">git.kernel.org/stable/c/1e3a3593162c96e8a8de48b1e14f60c3b57fca8a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/a2cd54b9348e485d338b3c132338a4410c99afaf">git.kernel.org/stable/c/a2cd54b9348e485d338b3c132338a4410c99afaf</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/6bce72daeccca9aa1746e92d6c3d4784e71f2ebb">git.kernel.org/stable/c/6bce72daeccca9aa1746e92d6c3d4784e71f2ebb</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/41b417ff73a24b2c68134992cc44c88db27f482d">git.kernel.org/stable/c/41b417ff73a24b2c68134992cc44c88db27f482d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

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 registered 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](https://cve.report/api)

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