



# netfilter: nf\_contrack\_h323: Add protection for bmp length out of range

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

## Summary

<b>CVE</b>	CVE-2024-26851
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-04-17 11:15:08 UTC
<b>Updated</b>	2026-05-12 12:16:20 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: netfilter: nf\_contrack\_h323: Add protection for bmp lengt

## 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-787

## 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 5e35941d990123f155b02d5663e51a24f816b6f3 98db42
CNA	Linux	Linux	affected 5e35941d990123f155b02d5663e51a24f816b6f3 4bafcc
CNA	Linux	Linux	affected 5e35941d990123f155b02d5663e51a24f816b6f3 ccd110
CNA	Linux	Linux	affected 5e35941d990123f155b02d5663e51a24f816b6f3 b3c0f5
CNA	Linux	Linux	affected 5e35941d990123f155b02d5663e51a24f816b6f3 39001e
CNA	Linux	Linux	affected 5e35941d990123f155b02d5663e51a24f816b6f3 014a8C
CNA	Linux	Linux	affected 5e35941d990123f155b02d5663e51a24f816b6f3 80ee5C
CNA	Linux	Linux	affected 5e35941d990123f155b02d5663e51a24f816b6f3 767146
CNA	Linux	Linux	affected 2.6.17
CNA	Linux	Linux	unaffected 2.6.17 semver
CNA	Linux	Linux	unaffected 4.19.310 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.272 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.213 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.152 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.82 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.22 6.6.* semver
CNA	Linux	Linux	unaffected 6.7.10 6.7.* semver
CNA	Linux	Linux	unaffected 6.8 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

## References

Reference	Source	Link
git.kernel.org/stable/c/80ee5054435a11c87c9a4f30f1ff750080c96416	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
lists.debian.org/debian-lts-announce/2024/06/msg00017.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
git.kernel.org/stable/c/39001e3c42000e7c2038717af0d33c32319ad591	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/014a807f1cc9c9d5173c1cd935835553b00d211c	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/767146637efc528b5e3d31297df115e85a2fd362	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/b3c0f553820516ad4b62a9390ecd28d6f73a7b13	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.co</a>

<a href="https://git.kernel.org/stable/c/4bafcc43baf7bcf93566394dbd15726b5b456b7a">git.kernel.org/stable/c/4bafcc43baf7bcf93566394dbd15726b5b456b7a</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/98db42191329c679f4ca52bec0b319689e1ad8cb">git.kernel.org/stable/c/98db42191329c679f4ca52bec0b319689e1ad8cb</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://lists.debian.org/debian-lts-announce/2024/06/msg00020.html">lists.debian.org/debian-lts-announce/2024/06/msg00020.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
<a href="https://git.kernel.org/stable/c/ccd1108b16ab572d9bf635586b0925635dbd6bbc">git.kernel.org/stable/c/ccd1108b16ab572d9bf635586b0925635dbd6bbc</a>	af854a3a-2127-422b-91ae-364da2661108	<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>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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)