



# net/smc: fix NULL dereference and UAF in smc\_tcp\_syn\_recv\_sock()

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

## Summary

<b>CVE</b>	CVE-2026-23450
<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 16:16:31 UTC
<b>Updated</b>	2026-04-18 09:16:27 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: net/smc: fix NULL dereference and UAF in smc\_tcp\_syn\_

## 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 ebfee3e153f67c8b38eb94a7062ee94aa6f92708 f315277856caefcd996c2611afc085ca2d53275 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8270d9c21041470f58348248b9d9dcf3bf79592e 1e4f873879e075bbd4eb1c644d6933303ac5eba4 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8270d9c21041470f58348248b9d9dcf3bf79592e f00fc26c8a06442b225a350fe000c0a11483e6a3 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8270d9c21041470f58348248b9d9dcf3bf79592e cadf3da46c15523fba90d80c9955f536ee3b4023 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8270d9c21041470f58348248b9d9dcf3bf79592e fd7579f0a2c84ba8a7d4f206201b50dc8ddf90c2 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8270d9c21041470f58348248b9d9dcf3bf79592e 1fab5ece76fb42a761178dcd0ebcbf578377b0dd git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8270d9c21041470f58348248b9d9dcf3bf79592e 6d5e4538364b9ceb1ac2941a4deb86650afb3538 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.18
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.18 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/cadf3da46c15523fba90d80c9955f536ee3b4023">git.kernel.org/stable/c/cadf3da46c15523fba90d80c9955f536ee3b4023</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/fd7579f0a2c84ba8a7d4f206201b50dc8ddf90c2">git.kernel.org/stable/c/fd7579f0a2c84ba8a7d4f206201b50dc8ddf90c2</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/1e4f873879e075bbd4eb1c644d6933303ac5eba4">git.kernel.org/stable/c/1e4f873879e075bbd4eb1c644d6933303ac5eba4</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/f315277856caefcd996c2611afc085ca2d53275">git.kernel.org/stable/c/f315277856caefcd996c2611afc085ca2d53275</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/6d5e4538364b9ceb1ac2941a4deb86650afb3538">git.kernel.org/stable/c/6d5e4538364b9ceb1ac2941a4deb86650afb3538</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/f00fc26c8a06442b225a350fe000c0a11483e6a3">git.kernel.org/stable/c/f00fc26c8a06442b225a350fe000c0a11483e6a3</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/1fab5ece76fb42a761178dcd0ebcbf578377b0dd">git.kernel.org/stable/c/1fab5ece76fb42a761178dcd0ebcbf578377b0dd</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>	canonic	
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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 registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**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)