



# bpf: Fix stack-out-of-bounds write in devmap

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

## Summary

<b>CVE</b>	CVE-2026-23359
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-25 11:16:34 UTC
<b>Updated</b>	2026-04-18 09:16:21 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: bpf: Fix stack-out-of-bounds write in devmap get\_upper\_if

## 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 aeea1b86f9363f3feabb496534d886f082a89f21 88df604f0d16a692867582350ce3f2fcd22243f1 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected aeea1b86f9363f3feabb496534d886f082a89f21 5000e40acc8d0c36ab709662e32120986ac22e7e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected aeea1b86f9363f3feabb496534d886f082a89f21 8a95fb9df1105b1618872c2846a6c01e3ba20b45 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected aeea1b86f9363f3feabb496534d886f082a89f21 d2c31d8e03d05edc16656e5ffe187f0d1da763d7 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected aeea1b86f9363f3feabb496534d886f082a89f21 75d474702b2ba8b6bcb26eb3004dbc5e95ffd5d2 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected aeea1b86f9363f3feabb496534d886f082a89f21 ca831567908fd3f73cf97d8a6c09a5054697a182 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected aeea1b86f9363f3feabb496534d886f082a89f21 b7bf516c3ecd9a2aae2dc2635178ab87b734fef1 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.15
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15 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 6.12.77 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.17 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.7 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/b7bf516c3ecd9a2aae2dc2635178ab87b734fef1">git.kernel.org/stable/c/b7bf516c3ecd9a2aae2dc2635178ab87b734fef1</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/88df604f0d16a692867582350ce3f2fcd22243f1">git.kernel.org/stable/c/88df604f0d16a692867582350ce3f2fcd22243f1</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/d2c31d8e03d05edc16656e5ffe187f0d1da763d7">git.kernel.org/stable/c/d2c31d8e03d05edc16656e5ffe187f0d1da763d7</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/8a95fb9df1105b1618872c2846a6c01e3ba20b45">git.kernel.org/stable/c/8a95fb9df1105b1618872c2846a6c01e3ba20b45</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ca831567908fd3f73cf97d8a6c09a5054697a182">git.kernel.org/stable/c/ca831567908fd3f73cf97d8a6c09a5054697a182</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/5000e40acc8d0c36ab709662e32120986ac22e7e">git.kernel.org/stable/c/5000e40acc8d0c36ab709662e32120986ac22e7e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/75d474702b2ba8b6bcb26eb3004dbc5e95ffd5d2">git.kernel.org/stable/c/75d474702b2ba8b6bcb26eb3004dbc5e95ffd5d2</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](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/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)