



bpf: support non-r10 register spill/fill to/from stack in precision tracking

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-52920
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-11-05 10:15:24 UTC
Updated	2026-05-17 16:16:13 UTC

Description In the Linux kernel, the following vulnerability has been resolved: bpf: support non-r10 register spill/fill to/from stack in prec

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

EPSS: 0.000150000 probability, percentile 0.030650000 (date 2026-05-17)

Problem Types: CWE-476

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 b5dc0163d8fd78e64a7e21f309cf932fda34353e ecc2aeaaa08a355d84d3ca9c3d2512399a194f29 git
CNA	Linux	Linux	affected b5dc0163d8fd78e64a7e21f309cf932fda34353e 199f0452873741fa4b8d4d88958e929030b2f92b git
CNA	Linux	Linux	affected b5dc0163d8fd78e64a7e21f309cf932fda34353e e4da60feca4d35e1a9b03dc0affa3354f9ff45e4 git
CNA	Linux	Linux	affected b5dc0163d8fd78e64a7e21f309cf932fda34353e 41f6f64e6999a837048b1bd13a2f8742964eca6b git
CNA	Linux	Linux	affected 5.3
CNA	Linux	Linux	unaffected 5.3 semver
CNA	Linux	Linux	unaffected 6.6.64 6.6.* semver
CNA	Linux	Linux	unaffected 6.6.70 6.6.* semver
CNA	Linux	Linux	unaffected 6.6.140 6.6.* semver
CNA	Linux	Linux	unaffected 6.8 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/41f6f64e6999a837048b1bd13a2f8742964eca6b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Mailing L
git.kernel.org/stable/c/ecc2aeaaa08a355d84d3ca9c3d2512399a194f29	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/199f0452873741fa4b8d4d88958e929030b2f92b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e4da60feca4d35e1a9b03dc0affa3354f9ff45e4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

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

CVE.report and Source URL Uptime Status status.cve.report