



xdp: fix invalid wait context of page_pool_destroy()

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

Summary

CVE	CVE-2024-43834
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-08-17 10:15:09 UTC
Updated	2026-05-12 12:17:07 UTC

Description In the Linux kernel, the following vulnerability has been resolved: xdp: fix invalid wait context of page_pool_destroy() If the c

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: NVD-CWE-noinfo

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 c3f812cea0d7006469d1cf33a4a9f0a12bb4b3a3 be9d08
CNA	Linux	Linux	affected c3f812cea0d7006469d1cf33a4a9f0a12bb4b3a3 6c390e
CNA	Linux	Linux	affected c3f812cea0d7006469d1cf33a4a9f0a12bb4b3a3 3fc1be3
CNA	Linux	Linux	affected c3f812cea0d7006469d1cf33a4a9f0a12bb4b3a3 bf0ce5a
CNA	Linux	Linux	affected c3f812cea0d7006469d1cf33a4a9f0a12bb4b3a3 121440
CNA	Linux	Linux	affected c3f812cea0d7006469d1cf33a4a9f0a12bb4b3a3 59a931
CNA	Linux	Linux	affected bf22306d92ca59c59dc4aa3bab14768948193d56 git
CNA	Linux	Linux	affected 05f646cb2174d1a4e032b60b99097f5c4b522616 git
CNA	Linux	Linux	affected 5.5
CNA	Linux	Linux	unaffected 5.5 semver
CNA	Linux	Linux	unaffected 5.10.224 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.165 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.103 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.44 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.3 6.10.* semver
CNA	Linux	Linux	unaffected 6.11 * 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/bf0ce5aa5f2525ed1b921ba36de96e458e77f482	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com
git.kernel.org/stable/c/12144069209eec7f2090ce9afa15acdcc2c2a537	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/3fc1be360b99baeea15cdee3cf94252cd3a72d26	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/59a931c5b732ca5fc2ca727f5a72aeabaafa85ec	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2024/10/msg00003.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/be9d08ff102df3ac4f66e826ea935cf3af63a4bd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/6c390ef198aa69795427a5cb5fd7cb4bc7e6cd7a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org

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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)