



net/bnx2x: Prevent access to a freed page in page_pool

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

Summary

CVE	CVE-2024-26859
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-17 11:15:08 UTC
Updated	2026-05-12 12:16:21 UTC

Description In the Linux kernel, the following vulnerability has been resolved: net/bnx2x: Prevent access to a freed page in page_pool

Risk And Classification

Primary CVSS: v3.1 4.7 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-362

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:H/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 4cace675d687ebd2d813e90af80ff87ee85202f9 7bcc09c
CNA	Linux	Linux	affected 4cace675d687ebd2d813e90af80ff87ee85202f9 4f37d3a
CNA	Linux	Linux	affected 4cace675d687ebd2d813e90af80ff87ee85202f9 8eebff9f
CNA	Linux	Linux	affected 4cace675d687ebd2d813e90af80ff87ee85202f9 8ffcd3cc
CNA	Linux	Linux	affected 4cace675d687ebd2d813e90af80ff87ee85202f9 cf7d8cb
CNA	Linux	Linux	affected 4cace675d687ebd2d813e90af80ff87ee85202f9 3a9f78b
CNA	Linux	Linux	affected 4cace675d687ebd2d813e90af80ff87ee85202f9 c51f8b6
CNA	Linux	Linux	affected 4cace675d687ebd2d813e90af80ff87ee85202f9 44f9f1a
CNA	Linux	Linux	affected 4cace675d687ebd2d813e90af80ff87ee85202f9 d27e2d
CNA	Linux	Linux	affected 4.2
CNA	Linux	Linux	unaffected 4.2 semver
CNA	Linux	Linux	unaffected 4.19.311 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.273 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.214 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.153 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.83 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.23 6.6.* semver
CNA	Linux	Linux	unaffected 6.7.11 6.7.* semver
CNA	Linux	Linux	unaffected 6.8.2 6.8.* semver
CNA	Linux	Linux	unaffected 6.9 * 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/8ffcd3ccbdba0c918c4a0f922ef1c17010f1b598	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/cf7d8cba639ae792a42c2a137b495eac262ac36c	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
lists.debian.org/debian-lts-announce/2024/06/msg00017.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/3a9f78b297e08ca8e88ae3ecff1f6fe2766dc5eb	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/8eebff95ce9558be66a36aa7cfb43223f3ab4699	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org

cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/44f9f1abb0ecc43023225ab9539167facbabf0ec	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/4f37d3a7e004bbf560c21441ca9c022168017ec4	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/7bcc090c81116c66936a7415f2c6b1483a4bcfd9	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/c51f8b6930db3f259b8820b589f2459d2df3fc68	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
lists.debian.org/debian-lts-announce/2024/06/msg00020.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/d27e2da94a42655861ca4baea30c8cd65546f25d	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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://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

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