



crypto: xilinx - call finalize with bh disabled

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

Summary

CVE	CVE-2024-26877
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-17 11:15:09 UTC
Updated	2026-05-12 12:16:22 UTC

Description In the Linux kernel, the following vulnerability has been resolved: crypto: xilinx - call finalize with bh disabled When calling 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 4d96f7d48131fefe30d7c1d1e2a23ef37164dbf5 8a01335
CNA	Linux	Linux	affected 4d96f7d48131fefe30d7c1d1e2a23ef37164dbf5 03e6d4e
CNA	Linux	Linux	affected 4d96f7d48131fefe30d7c1d1e2a23ef37164dbf5 a71f66b
CNA	Linux	Linux	affected 4d96f7d48131fefe30d7c1d1e2a23ef37164dbf5 23bc89f
CNA	Linux	Linux	affected 4d96f7d48131fefe30d7c1d1e2a23ef37164dbf5 9db89b1
CNA	Linux	Linux	affected 4d96f7d48131fefe30d7c1d1e2a23ef37164dbf5 dbf291d
CNA	Linux	Linux	affected 4d96f7d48131fefe30d7c1d1e2a23ef37164dbf5 a853450
CNA	Linux	Linux	affected 5.7
CNA	Linux	Linux	unaffected 5.7 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
lists.debian.org/debian-lts-announce/2024/06/msg00017.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/a71f66bd5f7b9b35a8aaa49e29565eca66299399	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.com
git.kernel.org/stable/c/8a01335aedc50a66d04dd39203c89f4bc8042596	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/03e6d4e948432a61b35783323b6ab2be071d2619	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/a853450bf4c752e664abab0b2fad395b7ad7701c	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/23bc89fdce71124cd2126fc919c7076e7cb489cf	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/dbf291d8ffffb70f48286176a15c6c54f0bb0743	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/9db89b1fb85557892e6681724b367287de5f9f20	af854a3a-2127-422b-91ae-364da2661108	git.kernel.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](#)