



net: usb: asix_devices: add phy_mask for ax88772 mdio bus

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

Summary

CVE	CVE-2025-38725
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-04 16:15:42 UTC
Updated	2026-05-12 13:17:02 UTC

Description In the Linux kernel, the following vulnerability has been resolved: net: usb: asix_devices: add phy_mask for ax88772 mdio b

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: 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 e532a096be0e5e570b383e71d4560e7f04384e0f 75947d3200de98a9ded9ad8972e02f1a1
CNA	Linux	Linux	affected e532a096be0e5e570b383e71d4560e7f04384e0f 59ed6fbd1bc03316e09493ffde7066f03
CNA	Linux	Linux	affected e532a096be0e5e570b383e71d4560e7f04384e0f ccef5ee4adf56472aa26bdd1f821a6d0cd
CNA	Linux	Linux	affected e532a096be0e5e570b383e71d4560e7f04384e0f ee2cd40b0bb46056949a2319084a729d
CNA	Linux	Linux	affected e532a096be0e5e570b383e71d4560e7f04384e0f a754ab53993b1585132e871c5d811167
CNA	Linux	Linux	affected e532a096be0e5e570b383e71d4560e7f04384e0f ad1f8313aeec0115f9978bd2d002ef4a8c
CNA	Linux	Linux	affected e532a096be0e5e570b383e71d4560e7f04384e0f 4faff70959d51078f9ee8372f8cff0d7045e
CNA	Linux	Linux	affected 5.14
CNA	Linux	Linux	unaffected 5.14 semver
CNA	Linux	Linux	unaffected 5.15.190 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.149 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.103 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.43 6.12.* semver
CNA	Linux	Linux	unaffected 6.15.11 6.15.* semver
CNA	Linux	Linux	unaffected 6.16.2 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/ccef5ee4adf56472aa26bdd1f821a6d0cd06089a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com
git.kernel.org/stable/c/ee2cd40b0bb46056949a2319084a729d95389386	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/59ed6fbd1bc03316e09493ffde7066f031c7524	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/4faff70959d51078f9ee8372f8cff0d7045e4114	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/ad1f8313aeec0115f9978bd2d002ef4a8d96c773	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/75947d3200de98a9ded9ad8972e02f1a177097fe	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/a754ab53993b1585132e871c5d811167ad3c52ff	416baaa9-dc9f-4396-8d5f-8c081fb06d67	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 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