



net: usb: asix_devices: Fix PHY address mask in MDIO bus initialization

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-38736 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2025-09-05 18:15:42 UTC |
| Updated | 2026-05-12 13:17:03 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: net: usb: asix_devices: Fix PHY address mask in MDIO bus initialization

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from nvd@nist.gov

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

Problem Types: CWE-125

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/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 75947d3200de98a9ded9ad8972e02f1a177097fe fcb4ce9f729c1d08e53abf9d449340e24c |
| CNA | Linux | Linux | affected 59ed6fbd1bc03316e09493fde7066f031c7524 8f141f2a4f2ef8ca865d5921574c3d6535e0 |
| CNA | Linux | Linux | affected ccef5ee4adf56472aa26bdd1f821a6d0cd06089a 748da80831221ae24b4bc8d7ffb22acd57 |
| CNA | Linux | Linux | affected ee2cd40b0bb46056949a2319084a729d95389386 22042ffedd8c2c6db08ccdd6d4273068e |
| CNA | Linux | Linux | affected ad1f8313aeec0115f9978bd2d002ef4a8d96c773 523eab02fce458fa6d3c51de5bb0558009 |
| CNA | Linux | Linux | affected 4faff70959d51078f9ee8372f8cff0d7045e4114 24ef2f53c07f273bad99173e27ee88d44d13f |
| CNA | Linux | Linux | affected a754ab53993b1585132e871c5d811167ad3c52ff git |
| CNA | Linux | Linux | affected 6.12.43 6.12.44 semver |
| CNA | Linux | Linux | affected 6.16.2 6.16.4 semver |
| 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/523eab02fce458fa6d3c51de5bb055800986953e | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/fcb4ce9f729c1d08e53abf9d449340e24c3edee6 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/22042ffedd8c2c6db08ccdd6d4273068eddd3c5c | 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/24ef2f53c07f273bad99173e27ee88d44d135b1c | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/8f141f2a4f2ef8ca865d5921574c3d6535e00a49 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/748da80831221ae24b4bc8d7ffb22acd5712a341 | 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](#)