net: phy: register phy led_triggers during probe to avoid AB-BA deadlock

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-23368
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 11:16:36 UTC
Updated	2026-04-18 09:16:21 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net: phy: register phy led_triggers during probe to avoid A

Risk And Classification

EPSS: 0.000320000 probability, percentile 0.090980000 (date 2026-04-18)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 06f502f57d0d7728f9fa0f157ec5e4111ddb98f6 2b01518eabace18f7ec8b4cafd52082303080dca git
CNA	Linux	Linux	affected 06f502f57d0d7728f9fa0f157ec5e4111ddb98f6 305afdd02ff3e694c165457793104710ec0728e5 git
CNA	Linux	Linux	affected 06f502f57d0d7728f9fa0f157ec5e4111ddb98f6 c6ffc2d2338d325e1edd0c702e3ee623aa5fdc6a git
CNA	Linux	Linux	affected 06f502f57d0d7728f9fa0f157ec5e4111ddb98f6 c33523b8fd2d4c504ada18cd93f511f2a8f84217 git
CNA	Linux	Linux	affected 06f502f57d0d7728f9fa0f157ec5e4111ddb98f6 241cd64cf2e32b28ead151b1795cd8fef2b6e482 git
CNA	Linux	Linux	affected 06f502f57d0d7728f9fa0f157ec5e4111ddb98f6 2764dcb3c35de4410f642afc62cf979727470575 git
CNA	Linux	Linux	affected 06f502f57d0d7728f9fa0f157ec5e4111ddb98f6 cde2d0b5ab5d03b5b6f17d4f654d8b30ccf36757 git
CNA	Linux	Linux	affected 06f502f57d0d7728f9fa0f157ec5e4111ddb98f6 c8dbdc6e380e7e96a51706db3e4b7870d8a9402d git
CNA	Linux	Linux	affected 4.16
CNA	Linux	Linux	unaffected 4.16 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.17 6.18.* semver

CNA	Linux	Linux	unaffected 6.19.7 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/2764dcb3c35de4410f642afc62cf979727470575	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c6ffc2d2338d325e1edd0c702e3ee623aa5fdc6a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/cde2d0b5ab5d03b5b6f17d4f654d8b30ccf36757	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c8dbdc6e380e7e96a51706db3e4b7870d8a9402d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c33523b8fd2d4c504ada18cd93f511f2a8f84217	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/305afdd02ff3e694c165457793104710ec0728e5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/241cd64cf2e32b28ead151b1795cd8fef2b6e482	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2b01518eabace18f7ec8b4cafd52082303080dca	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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 registred 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**