



media: solo6x10: Check for out of bounds chip_id

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

Summary

CVE	CVE-2026-43316
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 14:16:40 UTC
Updated	2026-05-12 14:10:27 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: media: solo6x10: Check for out of bounds chip_id Clang w

Risk And Classification

EPSS: 0.000240000 probability, percentile 0.070360000 (date 2026-05-12)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected faa4fd2a09517b39cc1f5d622453f97a59acfdac c327192ca26670cf6e588c1eeda66cd2fa97630e git
CNA	Linux	Linux	affected faa4fd2a09517b39cc1f5d622453f97a59acfdac 0b3dadada2417782a63ce32dae05bafe1c949e3f git
CNA	Linux	Linux	affected faa4fd2a09517b39cc1f5d622453f97a59acfdac 603e3859393ee2ce91393b7d05e6e56e4b66e5cd git
CNA	Linux	Linux	affected faa4fd2a09517b39cc1f5d622453f97a59acfdac 33af366211ee78e3b074ff44a16121e537e86826 git
CNA	Linux	Linux	affected faa4fd2a09517b39cc1f5d622453f97a59acfdac 5849ae68d7b8b6ad55cc1bf0d227dd2ae6362528 git
CNA	Linux	Linux	affected faa4fd2a09517b39cc1f5d622453f97a59acfdac d29f33b2cf98e4901cd5457d1ee34062e808df73 git
CNA	Linux	Linux	affected faa4fd2a09517b39cc1f5d622453f97a59acfdac 4d6db0c6bbbfd8d7bbdbf7ab6a9c003752abf1 16 git
CNA	Linux	Linux	affected faa4fd2a09517b39cc1f5d622453f97a59acfdac 0fdf6323c35a134f206dcad5babb4ff488552076 git
CNA	Linux	Linux	affected 2.6.36
CNA	Linux	Linux	unaffected 2.6.36 semver
CNA	Linux	Linux	unaffected 5.10.252 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.202 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.165 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.128 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/d29f33b2cf98e4901cd5457d1ee34062e808df73	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/4d6db0c6bbbfd8d7bbdbf7ab6a9c003752abf116	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/5849ae68d7b8b6ad55cc1bf0d227dd2ae6362528	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/0fdf6323c35a134f206dcad5babb4ff488552076	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/0b3dadada2417782a63ce32dae05bafec949e3f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/603e3859393ee2ce91393b7d05e6e56e4b66e5cd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/33af366211ee78e3b074ff44a16121e537e86826	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c327192ca26670cf6e588c1eeda66cd2fa97630e	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 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). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API cve.report/api

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