



x86/apic: Disable x2apic on resume if the kernel expects so

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

Summary

CVE	CVE-2026-43363
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:47 UTC
Updated	2026-05-08 15:16:47 UTC

Description In the Linux kernel, the following vulnerability has been resolved: x86/apic: Disable x2apic on resume if the kernel expects so

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 6e1cb38a2aef7680975e71f23de187859ee8b158 a6ad6f2e31b524cbb66b2f370bad0cf17d327e6c git
CNA	Linux	Linux	affected 6e1cb38a2aef7680975e71f23de187859ee8b158 3dd0812a7c764cd8f3b0182441ac22da0a7f3b09 git
CNA	Linux	Linux	affected 6e1cb38a2aef7680975e71f23de187859ee8b158 965289b120cc68cca886c75219c68b8c15751d73 gi
CNA	Linux	Linux	affected 6e1cb38a2aef7680975e71f23de187859ee8b158 f591938072115bf08730b8530c67fab189cc6308 git
CNA	Linux	Linux	affected 6e1cb38a2aef7680975e71f23de187859ee8b158 1a85f84214f9d790216547ac6086bf8033cd9e5a git
CNA	Linux	Linux	affected 6e1cb38a2aef7680975e71f23de187859ee8b158 11712c4eb384098db4cb08792e223c818b908c1a g
CNA	Linux	Linux	affected 6e1cb38a2aef7680975e71f23de187859ee8b158 1d8440c1e7c49715f937416ac90cf260f1f1712c git
CNA	Linux	Linux	affected 6e1cb38a2aef7680975e71f23de187859ee8b158 8cc7dd77a1466f0ec58c03478b2e735a5b289b96 gi
CNA	Linux	Linux	affected 2.6.28
CNA	Linux	Linux	unaffected 2.6.28 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 6.18.19 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.9 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/f591938072115bf08730b8530c67fab189cc6308	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/11712c4eb384098db4cb08792e223c818b908c1a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1d8440c1e7c49715f937416ac90cf260f1f1712c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/3dd0812a7c764cd8f3b0182441ac22da0a7f3b09	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8cc7dd77a1466f0ec58c03478b2e735a5b289b96	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1a85f84214f9d790216547ac6086bf8033cd9e5a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a6ad6f2e31b524cbb66b2f370bad0cf17d327e6c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/965289b120cc68cca886c75219c68b8c15751d73	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](https://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/cve). 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