



# cpufreq: governor: fix double free in cpufreq\_dbs\_governor\_init() error path

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

## Summary

<b>CVE</b>	CVE-2026-43328
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-08 14:16:42 UTC
<b>Updated</b>	2026-05-12 14:10:27 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: cpufreq: governor: fix double free in cpufreq\_dbs\_governor

## Risk And Classification

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

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4ebe36c94aed95de71a8ce6a6762226d31c938ee 56bc91ee78babe9578585a2bc137abc4b3115ff3 g
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4ebe36c94aed95de71a8ce6a6762226d31c938ee 019ea28629720c220daedf38107c8787f330dc05 g
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4ebe36c94aed95de71a8ce6a6762226d31c938ee da39ee627fd82b52068d4d5f115749a8b7d271f9 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4ebe36c94aed95de71a8ce6a6762226d31c938ee 427d048e4f6acbfa01b5a8062449fe0ee8987c0d gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4ebe36c94aed95de71a8ce6a6762226d31c938ee d2703b4f8fb7cc6f0dfdb2dc2359cc46189e7357 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4ebe36c94aed95de71a8ce6a6762226d31c938ee 3bf9d023d2329a0e5379f2fd09d06ef09729cd9d git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4ebe36c94aed95de71a8ce6a6762226d31c938ee 6dcf9d0064ce2f3e3dfe5755f98b93abe6a98e1e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e977b1477a6725868302957e6b5c330220391797 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.2
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.2 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10.253 5.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.168 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.134 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.81 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.22 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.12 6.19.* semver

## References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/427d048e4f6acbfa01b5a8062449fe0ee8987c0d">git.kernel.org/stable/c/427d048e4f6acbfa01b5a8062449fe0ee8987c0d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/d2703b4f8fb7cc6f0dfdb2dc2359cc46189e7357">git.kernel.org/stable/c/d2703b4f8fb7cc6f0dfdb2dc2359cc46189e7357</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/56bc91ee78babe9578585a2bc137abc4b3115ff3">git.kernel.org/stable/c/56bc91ee78babe9578585a2bc137abc4b3115ff3</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/6dcf9d0064ce2f3e3dfe5755f98b93abe6a98e1e">git.kernel.org/stable/c/6dcf9d0064ce2f3e3dfe5755f98b93abe6a98e1e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/019ea28629720c220daedf38107c8787f330dc05">git.kernel.org/stable/c/019ea28629720c220daedf38107c8787f330dc05</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/da39ee627fd82b52068d4d5f115749a8b7d271f9">git.kernel.org/stable/c/da39ee627fd82b52068d4d5f115749a8b7d271f9</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/3bf9d023d2329a0e5379f2fd09d06ef09729cd9d">git.kernel.org/stable/c/3bf9d023d2329a0e5379f2fd09d06ef09729cd9d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonica

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/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)