



# spi: fix use-after-free on controller registration failure

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

## Summary

<b>CVE</b>	CVE-2026-31389
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-03 16:16:36 UTC
<b>Updated</b>	2026-04-03 16:16:36 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: spi: fix use-after-free on controller registration failure Make

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6598b91b5ac32bc756d7c3000a31f775d4ead1c4 0e23f50086da7d0b183dfeac26021acfcdee086b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6598b91b5ac32bc756d7c3000a31f775d4ead1c4 6bbd385b30c7fb6c7ee0669e9ada91490938c051 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6598b91b5ac32bc756d7c3000a31f775d4ead1c4 afe27c1f43aa57530011f419be6ddf71306565d2 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6598b91b5ac32bc756d7c3000a31f775d4ead1c4 80f3e8cd2b4ad355b2ad2024cf423f6d183404f7 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6598b91b5ac32bc756d7c3000a31f775d4ead1c4 23b51bad2eb8787aa74324fccefb258515ae5ba git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6598b91b5ac32bc756d7c3000a31f775d4ead1c4 8634e05b08ead636e926022f4a98416e13440df9 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.0
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.0 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.167 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.130 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.78 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.20 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.10 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0-rc5 * original_commit_for_fix

## References

Reference	Source	Link	Tags
git.kernel.org/stable/c/6bbd385b30c7fb6c7ee0669e9ada91490938c051	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/afe27c1f43aa57530011f419be6ddf71306565d2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/23b51bad2eb8787aa74324fccefb258515ae5ba	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	

git.kernel.org/stable/c/80f3e8cd2b4ad355b2ad2024cf423f6d183404f7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/8634e05b08ead636e926022f4a98416e13440df9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/0e23f50086da7d0b183dfeac26021acfcdee086b	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>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

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](https://www.mitre.org/licenses).

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