



# sched\_ext: Disable preemption between scx\_claim\_exit() and kicking helper work

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

## Summary

<b>CVE</b>	CVE-2026-43482
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-13 16:16:51 UTC
<b>Updated</b>	2026-05-13 16:16:51 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: sched\_ext: Disable preemption between scx\_claim\_exit()

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f0e1a0643a59bf1f922fa209cec86a170b784f3f 41423912f7ac7494ccd6eef411227b4efce740e0 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f0e1a0643a59bf1f922fa209cec86a170b784f3f 522acaae34aa7e05859260056b39c7c030592a0c git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f0e1a0643a59bf1f922fa209cec86a170b784f3f 5131dbec2c10961b34f844bc30b400c3fa0bcc72 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f0e1a0643a59bf1f922fa209cec86a170b784f3f 83236b2e43dba00bee5b82eb5758816b1a674f6a git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.12
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12 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 6.19.9 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/41423912f7ac7494ccd6eef411227b4efce740e0">git.kernel.org/stable/c/41423912f7ac7494ccd6eef411227b4efce740e0</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/522acaae34aa7e05859260056b39c7c030592a0c">git.kernel.org/stable/c/522acaae34aa7e05859260056b39c7c030592a0c</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/83236b2e43dba00bee5b82eb5758816b1a674f6a">git.kernel.org/stable/c/83236b2e43dba00bee5b82eb5758816b1a674f6a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/5131dbec2c10961b34f844bc30b400c3fa0bcc72">git.kernel.org/stable/c/5131dbec2c10961b34f844bc30b400c3fa0bcc72</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>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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](#) 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](#)