



# net/sched: sch\_hfsc: fix divide-by-zero in rtsc\_min()

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

## Summary

<b>CVE</b>	CVE-2026-31423
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-13 14:16:12 UTC
<b>Updated</b>	2026-04-18 09:16:32 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_hfsc: fix divide-by-zero in rtsc_min() m2sr

## Risk And Classification

**EPSS:** 0.000240000 probability, percentile 0.066100000 (date 2026-04-18)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 ad8e8fec40290a8c8cf145c0deaadf76f80c5163 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 ab1ff5890c7354afc7be56502fcfbd61f3b7ae4f git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 25b6821884713a31e2b49fb67b0ebd765b33e0a9 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 c56f78614e7781aaceca9bd3cb2128bf7d45c3bd git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 b9e6431cbea8bb1fae8069ed099b4ee100499835 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 17c1b9807b8a67d676b6dcf749ee932ebaa7f568 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 d0aefec1b1a1ba2c1d251028dc2c4e5b4ce1fea5 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 4576100b8cd03118267513cafacde164b498b322 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 2.6.12
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 2.6.12 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 5.15.203 5.15.* 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/c56f78614e7781aaceca9bd3cb2128bf7d45c3bd">git.kernel.org/stable/c/c56f78614e7781aaceca9bd3cb2128bf7d45c3bd</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ad8e8fec40290a8c8cf145c0deaadf76f80c5163">git.kernel.org/stable/c/ad8e8fec40290a8c8cf145c0deaadf76f80c5163</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/b9e6431cbea8bb1fae8069ed099b4ee100499835">git.kernel.org/stable/c/b9e6431cbea8bb1fae8069ed099b4ee100499835</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/25b6821884713a31e2b49fb67b0ebd765b33e0a9">git.kernel.org/stable/c/25b6821884713a31e2b49fb67b0ebd765b33e0a9</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ab1ff5890c7354afc7be56502fcfd61f3b7ae4f">git.kernel.org/stable/c/ab1ff5890c7354afc7be56502fcfd61f3b7ae4f</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/17c1b9807b8a67d676b6dcf749ee932ebaa7f568">git.kernel.org/stable/c/17c1b9807b8a67d676b6dcf749ee932ebaa7f568</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/4576100b8cd03118267513cafacde164b498b322">git.kernel.org/stable/c/4576100b8cd03118267513cafacde164b498b322</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/d0aefec1b1a1ba2c1d251028dc2c4e5b4ce1fea5">git.kernel.org/stable/c/d0aefec1b1a1ba2c1d251028dc2c4e5b4ce1fea5</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](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/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)