



# scsi: mpi3mr: Add NULL checks when resetting request and reply queues

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

## Summary

<b>CVE</b>	CVE-2026-43473
<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 15:17:00 UTC
<b>Updated</b>	2026-05-09 06:16:15 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: scsi: mpi3mr: Add NULL checks when resetting request and reply queues

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fe6db615156573d3f6a37564b8a590cb03bbaf25 7df0296ad4e9253d12c6dbe7f120044dddc95600 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fe6db615156573d3f6a37564b8a590cb03bbaf25 7da755e0d02e9ca035065127e108d1fed8950dc8 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fe6db615156573d3f6a37564b8a590cb03bbaf25 78d3f201f8b609928eade53cf03a52df5415aaf7 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fe6db615156573d3f6a37564b8a590cb03bbaf25 e978a36f332ede78eb4de037b517db16265d420d git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fe6db615156573d3f6a37564b8a590cb03bbaf25 220d7ca70611a73d50ef8e9edac630ed1ecec7c git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected fe6db615156573d3f6a37564b8a590cb03bbaf25 fa96392ebebcb8fade2b878acb14cce0f71016503 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.17
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.17 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 6.18.19 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
git.kernel.org/stable/c/fa96392ebebcb8fade2b878acb14cce0f71016503	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/7da755e0d02e9ca035065127e108d1fed8950dc8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	

<a href="https://git.kernel.org/stable/c/78d3f201f8b609928eade53cf03a52df5415aaf7">git.kernel.org/stable/c/78d3f201f8b609928eade53cf03a52df5415aaf7</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/7df0296ad4e9253d12c6dbe7f120044dddc95600">git.kernel.org/stable/c/7df0296ad4e9253d12c6dbe7f120044dddc95600</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/220d7ca70611a73d50ef8e9edac630ed1ecec7c">git.kernel.org/stable/c/220d7ca70611a73d50ef8e9edac630ed1ecec7c</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/e978a36f332ede78eb4de037b517db16265d420d">git.kernel.org/stable/c/e978a36f332ede78eb4de037b517db16265d420d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/f8e833572a3e12a2a1ffe7b3646af024264d38ca">git.kernel.org/stable/c/f8e833572a3e12a2a1ffe7b3646af024264d38ca</a>	MITRE	<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)