



# remoteproc: imx\_rproc: Fix invalid loaded resource table detection

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

## Summary

<b>CVE</b>	CVE-2026-43145
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 12:16:31 UTC
<b>Updated</b>	2026-05-06 13:07:51 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: remoteproc: imx\_rproc: Fix invalid loaded resource table c

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 64f2ca5ce97111a364a18c31772eb46c79e8b772 91baf24d972ea3c04a75dd18821c03d223c0dbc0 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1d750606fedcddf7886f35a558c51b05ce2680a6 fcec79b6a3649ae7b1f659267602ca402c240d6e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 7fb5f957213bc7268bac449f8bfe95967c9f3f3b 9bd98d088f47153a81a6ec8162b4415c64aa7f39 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e954a1bd16102abc800629f9900715d8ec4c3130 65379adf7d231c930572db45933ff4538f4c5128 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e954a1bd16102abc800629f9900715d8ec4c3130 500778df9e4c313190368908ff40c23948508e97 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e954a1bd16102abc800629f9900715d8ec4c3130 198c629bd03863591f3fbf5ce8ff974a33f13dc9 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e954a1bd16102abc800629f9900715d8ec4c3130 26aa5295010ffaebcf8f1991c53fa7cf2ee1b20d git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3d131f138e092c414c69860f2c897c59d660da99 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 5.15.202 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.165 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.128 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.75 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.16 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.6 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/91baf24d972ea3c04a75dd18821c03d223c0dbc0">git.kernel.org/stable/c/91baf24d972ea3c04a75dd18821c03d223c0dbc0</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/9bd98d088f47153a81a6ec8162b4415c64aa7f39">git.kernel.org/stable/c/9bd98d088f47153a81a6ec8162b4415c64aa7f39</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/26aa5295010ffaebcf8f1991c53fa7cf2ee1b20d">git.kernel.org/stable/c/26aa5295010ffaebcf8f1991c53fa7cf2ee1b20d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/500778df9e4c313190368908ff40c23948508e97">git.kernel.org/stable/c/500778df9e4c313190368908ff40c23948508e97</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/65379adf7d231c930572db45933ff4538f4c5128">git.kernel.org/stable/c/65379adf7d231c930572db45933ff4538f4c5128</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/fcec79b6a3649ae7b1f659267602ca402c240d6e">git.kernel.org/stable/c/fcec79b6a3649ae7b1f659267602ca402c240d6e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/198c629bd03863591f3fbf5ce8ff974a33f13dc9">git.kernel.org/stable/c/198c629bd03863591f3fbf5ce8ff974a33f13dc9</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>	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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://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)