



# scsi: ibmvfc: Fix OOB access in `ibmvfc_discover_targets_done()`

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

## Summary

<b>CVE</b>	CVE-2026-31464
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-22 14:16:42 UTC
<b>Updated</b>	2026-04-22 14:16:42 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: scsi: ibmvfc: Fix OOB access in `ibmvfc_discover_targets`

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 072b91f9c6510d0ec4a49d07dbc318760c7da7b3 d842348f8a00d5b1d7358f207eb34ffc5b16df3 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 072b91f9c6510d0ec4a49d07dbc318760c7da7b3 a007246cb6c9ebdc93dafbf63cc2d43d98f402cc git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 072b91f9c6510d0ec4a49d07dbc318760c7da7b3 394a1cac3c12fdd7d77f19ccfd222ab5ff87ef89 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 072b91f9c6510d0ec4a49d07dbc318760c7da7b3 4ed727e35b0ab17d3eeeb1e8023768396e2be161 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 072b91f9c6510d0ec4a49d07dbc318760c7da7b3 d1466bf991b2343cf2ba8336e440c8faf3cbb780 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 072b91f9c6510d0ec4a49d07dbc318760c7da7b3 786f10b1966e485046839f992e89f2c18cbd1983 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 072b91f9c6510d0ec4a49d07dbc318760c7da7b3 bae4df0a643fa7f84663473aa3082a9c2ed139db git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 072b91f9c6510d0ec4a49d07dbc318760c7da7b3 61d099ac4a7a8fb11ebdb6e2ec8d77f38e77362f git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 2.6.27
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 2.6.27 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 6.6.131 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.80 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.21 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.11 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/a007246cb6c9ebdc93dafbf63cc2d43d98f402cc">git.kernel.org/stable/c/a007246cb6c9ebdc93dafbf63cc2d43d98f402cc</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/394a1cac3c12fdd7d77f19ccfd222ab5ff87ef89">git.kernel.org/stable/c/394a1cac3c12fdd7d77f19ccfd222ab5ff87ef89</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/4ed727e35b0ab17d3eeeb1e8023768396e2be161">git.kernel.org/stable/c/4ed727e35b0ab17d3eeeb1e8023768396e2be161</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/d842348f8a00d5b1d7358f207eb34ffc5b16df3">git.kernel.org/stable/c/d842348f8a00d5b1d7358f207eb34ffc5b16df3</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/bae4df0a643fa7f84663473aa3082a9c2ed139db">git.kernel.org/stable/c/bae4df0a643fa7f84663473aa3082a9c2ed139db</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/d1466bf991b2343cf2ba8336e440c8faf3cbb780">git.kernel.org/stable/c/d1466bf991b2343cf2ba8336e440c8faf3cbb780</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/61d099ac4a7a8fb11ebdb6e2ec8d77f38e77362f">git.kernel.org/stable/c/61d099ac4a7a8fb11ebdb6e2ec8d77f38e77362f</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/786f10b1966e485046839f992e89f2c18cbd1983">git.kernel.org/stable/c/786f10b1966e485046839f992e89f2c18cbd1983</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](#).

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)