



cxl/port: Fix use after free of parent_port in cxl_detach_ep()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-31530
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 14:16:53 UTC
Updated	2026-04-22 14:16:53 UTC

Description In the Linux kernel, the following vulnerability has been resolved: cxl/port: Fix use after free of parent_port in cxl_detach_ep

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 2345df54249c6fb7779e2a72b427ee79ed3eaad5 d216a4bd138eb57cc4ae7c43b2f709e3482af7e2 git
CNA	Linux	Linux	affected 2345df54249c6fb7779e2a72b427ee79ed3eaad5 2c32141462045cf93d54a5146a0ba572b83533dd git
CNA	Linux	Linux	affected 2345df54249c6fb7779e2a72b427ee79ed3eaad5 f7dc6f381a1e5f068333f1faa9265d6af1df4235 git
CNA	Linux	Linux	affected 2345df54249c6fb7779e2a72b427ee79ed3eaad5 19d2f0b97a131198efc2c4ca3eb7f980bba8c2b4 git
CNA	Linux	Linux	affected 6.3
CNA	Linux	Linux	unaffected 6.3 semver
CNA	Linux	Linux	unaffected 6.12.80 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.21 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.11 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/2c32141462045cf93d54a5146a0ba572b83533dd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d216a4bd138eb57cc4ae7c43b2f709e3482af7e2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/19d2f0b97a131198efc2c4ca3eb7f980bba8c2b4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f7dc6f381a1e5f068333f1faa9265d6af1df4235	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	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](#)