



io_uring/zcrx: fix post open error handling

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2026-43174
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:35 UTC
Updated	2026-05-12 20:01:34 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: io_uring/zcrx: fix post open error handling Closing a queue

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.000240000 probability, percentile 0.069290000 (date 2026-05-12)

Problem Types: NVD-CWE-noinfo

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products			
Source	Vendor	Product	Version
CNA	Linux	Linux	affected e0793de24a9f610bd8ce106f7033b3966e7fca0e 18afaff077b46655a8eb6fd7f6de1b81327be577 git
CNA	Linux	Linux	affected e0793de24a9f610bd8ce106f7033b3966e7fca0e 5d540e4508950c674d6feef1d95463d039bbf4f5 git
CNA	Linux	Linux	affected 6.15
CNA	Linux	Linux	unaffected 6.15 semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References			
Reference	Source	Link	Tags
git.kernel.org/stable/c/5d540e4508950c674d6feef1d95463d039bbf4f5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/18afaff077b46655a8eb6fd7f6de1b81327be577	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.