



io_uring/io-wq: check IO_WQ_BIT_EXIT inside work run loop

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

Summary

CVE	CVE-2026-23113
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-14 15:16:06 UTC
Updated	2026-04-18 09:16:14 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: io_uring/io-wq: check IO_WQ_BIT_EXIT inside work run l

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

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 c60eb049f4a19dddddcd3ee97a9c79ab8066a6a03 27e47500fac23d15b7dc93ff650bc4844d2581bd git
CNA	Linux	Linux	affected c60eb049f4a19dddddcd3ee97a9c79ab8066a6a03 d05d99573f81a091547b1778b9a50120f5d6c68a gi
CNA	Linux	Linux	affected c60eb049f4a19dddddcd3ee97a9c79ab8066a6a03 85eb83694a91c89d9abe615d717c0053c3efa714 g
CNA	Linux	Linux	affected c60eb049f4a19dddddcd3ee97a9c79ab8066a6a03 2e8ca1078b14142db2ce51cbd18ff9971560046b git
CNA	Linux	Linux	affected c60eb049f4a19dddddcd3ee97a9c79ab8066a6a03 bdf0bf73006ea8af9327cdb85cfdff4c23a5f966 git
CNA	Linux	Linux	affected c60eb049f4a19dddddcd3ee97a9c79ab8066a6a03 10dc959398175736e495f71c771f8641e1ca1907 git
CNA	Linux	Linux	affected 5.12
CNA	Linux	Linux	unaffected 5.12 semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.122 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.68 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.8 6.18.* semver
CNA	Linux	Linux	unaffected 6.19 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/d05d99573f81a091547b1778b9a50120f5d6c68a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/27e47500fac23d15b7dc93ff650bc4844d2581bd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/10dc959398175736e495f71c771f8641e1ca1907	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/85eb83694a91c89d9abe615d717c0053c3efa714	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/bdf0bf73006ea8af9327cdb85cfdff4c23a5f966	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/2e8ca1078b14142db2ce51cbd18ff9971560046b	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.

© [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](#)