espintcp: Fix race condition in espintcp_close()

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-23239
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-10 18:18:13 UTC
Updated	2026-04-02 15:16:25 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: espintcp: Fix race condition in espintcp_close() This issue

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000130000 probability, percentile 0.022850000 (date 2026-04-07)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected e27cca96cd68fa2c6814c90f9a1cfd36bb68c593 f7ad8b1d0e421c524604d5076b73232093490d5c git
CNA	Linux	Linux	affected e27cca96cd68fa2c6814c90f9a1cfd36bb68c593 664e9df53226b4505a0894817ecad2c610ab11d8 git
CNA	Linux	Linux	affected e27cca96cd68fa2c6814c90f9a1cfd36bb68c593 022ff7f347588de6e17879a1da6019647b21321b git
CNA	Linux	Linux	affected e27cca96cd68fa2c6814c90f9a1cfd36bb68c593 e1512c1db9e8794d8d130addd2615ec27231d994 git
CNA	Linux	Linux	affected 5.6
CNA	Linux	Linux	unaffected 5.6 semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0-rc2 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/f7ad8b1d0e421c524604d5076b73232093490d5c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/022ff7f347588de6e17879a1da6019647b21321b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/664e9df53226b4505a0894817ecad2c610ab11d8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e1512c1db9e8794d8d130addd2615ec27231d994	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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**