



mailbox: mchp-ipc-sbi: fix out-of-bounds access in mchp_ipc_get_cluster_aggr_irq()

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

Summary

CVE	CVE-2026-43274
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:48 UTC
Updated	2026-05-08 19:31:52 UTC

Description In the Linux kernel, the following vulnerability has been resolved: mailbox: mchp-ipc-sbi: fix out-of-bounds access in mchp_i

Risk And Classification

Primary CVSS: v3.1 8.4 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000120000 probability, percentile 0.016960000 (date 2026-05-09)

Problem Types: CWE-125

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/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 e4b1d67e71419c4af581890ecea84b04920d4116 95438699c92947155823dcd3918049a07f3cd867 g
CNA	Linux	Linux	affected e4b1d67e71419c4af581890ecea84b04920d4116 0442b6229e2eedc95a6d3d18ce75dec7f5b5377c g
CNA	Linux	Linux	affected e4b1d67e71419c4af581890ecea84b04920d4116 f7c330a8c83c9b0332fd524097eaf3e69148164d git
CNA	Linux	Linux	affected 6.14
CNA	Linux	Linux	unaffected 6.14 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 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/95438699c92947155823dcd3918049a07f3cd867	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f7c330a8c83c9b0332fd524097eaf3e69148164d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/0442b6229e2eedc95a6d3d18ce75dec7f5b5377c	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.

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