



ACPI: EC: clean up handlers on probe failure in acpi_ec_setup()

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

Summary

CVE	CVE-2026-31426
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 14:16:12 UTC
Updated	2026-04-13 15:01:43 UTC

Description In the Linux kernel, the following vulnerability has been resolved: ACPI: EC: clean up handlers on probe failure in acpi_ec_s

Risk And Classification

EPSS: 0.000240000 probability, percentile 0.066090000 (date 2026-04-15)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 03e9a0e05739cf872fee494b06c75c0469704a21 022d1727f33ff90b3e1775125264e3023901952e git
CNA	Linux	Linux	affected 03e9a0e05739cf872fee494b06c75c0469704a21 9c886e63b69658959633937e3acb7ca8addf7499 git
CNA	Linux	Linux	affected 03e9a0e05739cf872fee494b06c75c0469704a21 808c0f156f48d5b8ca34088cbbfba8444e606cbc git
CNA	Linux	Linux	affected 03e9a0e05739cf872fee494b06c75c0469704a21 d04c007047c88158141d9bd5eac761cdadd3782c git
CNA	Linux	Linux	affected 03e9a0e05739cf872fee494b06c75c0469704a21 be1a827e15991e874e0d5222d0ea5fdad01960fe git
CNA	Linux	Linux	affected 03e9a0e05739cf872fee494b06c75c0469704a21 f6484cadbcacf26b5844b51bd7307a663dda48ef6 git
CNA	Linux	Linux	affected 5.7
CNA	Linux	Linux	unaffected 5.7 semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.131 6.6.* 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/808c0f156f48d5b8ca34088cbbfba8444e606cbc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d04c007047c88158141d9bd5eac761cdadd3782c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/be1a827e15991e874e0d5222d0ea5fdad01960fe	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/022d1727f33ff90b3e1775125264e3023901952e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9c886e63b69658959633937e3acb7ca8addf7499	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f6484cadbcaf26b5844b51bd7307a663dda48ef6	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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API cve.report/api

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