



# EFI/CPER: don't go past the ARM processor CPER record buffer

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

## Summary

<b>CVE</b>	CVE-2026-43266
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 12:16:47 UTC
<b>Updated</b>	2026-05-06 13:07:51 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: EFI/CPER: don't go past the ARM processor CPER record buffer

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 c80113dcfc807308f5ab33847fae77e07531aeb8 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 ca2aad8771aa9091bc9e42e7d546bd40b72ddcd4 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 a68d22902a6916e10ee235fee609239004e129d0 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 64eb63f573f497553e1a0c388bbcdd639e0f0704 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 be10c1bdf64a39832998f54900aa309b3917abcf git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 25b290624b0e3d2f0f90238709ee0b6009b9fde8 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 45766863baf899059e75595dd3cb1116467f2095 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 eae21beecb95a3b69ee5c38a659f774e171d730e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10.252 5.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15.202 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.165 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.128 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.75 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.16 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.6 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
-----------	--------	------	------

<a href="https://git.kernel.org/stable/c/64eb63f573f497553e1a0c388bbcdd639e0f0704">git.kernel.org/stable/c/64eb63f573f497553e1a0c388bbcdd639e0f0704</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/a68d22902a6916e10ee235fee609239004e129d0">git.kernel.org/stable/c/a68d22902a6916e10ee235fee609239004e129d0</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/eae21beecb95a3b69ee5c38a659f774e171d730e">git.kernel.org/stable/c/eae21beecb95a3b69ee5c38a659f774e171d730e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/25b290624b0e3d2f0f90238709ee0b6009b9fde8">git.kernel.org/stable/c/25b290624b0e3d2f0f90238709ee0b6009b9fde8</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/be10c1bdf64a39832998f54900aa309b3917abcf">git.kernel.org/stable/c/be10c1bdf64a39832998f54900aa309b3917abcf</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/c80113dcfc807308f5ab33847fae77e07531aeb8">git.kernel.org/stable/c/c80113dcfc807308f5ab33847fae77e07531aeb8</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/45766863baf899059e75595dd3cb1116467f2095">git.kernel.org/stable/c/45766863baf899059e75595dd3cb1116467f2095</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/ca2aad8771aa9091bc9e42e7d546bd40b72ddcd4">git.kernel.org/stable/c/ca2aad8771aa9091bc9e42e7d546bd40b72ddcd4</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a> canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a> 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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)