



crypto: authencesn - Do not place hiseq at end of dst for out-of-place decryption

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

Summary

CVE	CVE-2026-43033
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 15:16:47 UTC
Updated	2026-05-01 15:24:14 UTC

Description In the Linux kernel, the following vulnerability has been resolved: crypto: authencesn - Do not place hiseq at end of dst for

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 104880a6b470958ddc30e139c41aa4f6ed3a5234 8c62f618576519dbed6816fafc623ce592953025 git
CNA	Linux	Linux	affected 104880a6b470958ddc30e139c41aa4f6ed3a5234 d589abd8b019b07075fda255ceab8c8e950cdb3f git
CNA	Linux	Linux	affected 104880a6b470958ddc30e139c41aa4f6ed3a5234 5466e7d0cd9e4f9cef9d8f18f18b60e7bc1c77e5 git
CNA	Linux	Linux	affected 104880a6b470958ddc30e139c41aa4f6ed3a5234 d0c4ff6812386880f30bc64c2921299cc4d7b47f git
CNA	Linux	Linux	affected 104880a6b470958ddc30e139c41aa4f6ed3a5234 89fe118b6470119b20c04afc36e45b81a69ea11f git
CNA	Linux	Linux	affected 104880a6b470958ddc30e139c41aa4f6ed3a5234 153d5520c3f9fd62e71c7e7f9e34b59cf411e555 git
CNA	Linux	Linux	affected 104880a6b470958ddc30e139c41aa4f6ed3a5234 cded4002d22177e8deaca1f257ecd932c9582b6b g
CNA	Linux	Linux	affected 104880a6b470958ddc30e139c41aa4f6ed3a5234 e02494114ebf7c8b42777c6cd6982f113bfdbec7 git
CNA	Linux	Linux	affected 4.3
CNA	Linux	Linux	unaffected 4.3 semver
CNA	Linux	Linux	unaffected 5.10.254 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.204 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.170 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.137 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.85 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.22 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.12 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/d0c4ff6812386880f30bc64c2921299cc4d7b47f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e02494114ebf7c8b42777c6cd6982f113bfdbec7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8c62f618576519dbed6816fafc623ce592953025	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/89fe118b6470119b20c04afc36e45b81a69ea11f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/5466e7d0cd9e4f9cef9d8f18f18b60e7bc1c77e5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d589abd8b019b07075fda255ceab8c8e950cdb3f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/153d5520c3f9fd62e71c7e7f9e34b59cf411e555	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/cded4002d22177e8deaca1f257ecd932c9582b6b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
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](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/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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