



crypto: krb5enc - fix async decrypt skipping hash verification

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

Summary

CVE	CVE-2026-31719
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:22 UTC
Updated	2026-05-03 07:16:19 UTC

Description In the Linux kernel, the following vulnerability has been resolved: crypto: krb5enc - fix async decrypt skipping hash verification

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000170000 probability, percentile 0.040880000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected d1775a177f7f38156d541c8a3e3c91eaa6e69699 07cbb1bd424370671814a862913c99a6e1441588 g
CNA	Linux	Linux	affected d1775a177f7f38156d541c8a3e3c91eaa6e69699 e51f42114abddf47f29dda43e7826be28907fcd2 git
CNA	Linux	Linux	affected d1775a177f7f38156d541c8a3e3c91eaa6e69699 3bfbf5f0a99c991769ec562721285df7ab69240b git
CNA	Linux	Linux	affected 6.15
CNA	Linux	Linux	unaffected 6.15 semver
CNA	Linux	Linux	unaffected 6.18.25 6.18.* semver
CNA	Linux	Linux	unaffected 7.0.2 7.0.* semver
CNA	Linux	Linux	unaffected 7.1-rc1 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/e51f42114abddf47f29dda43e7826be28907fcd2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/07cbb1bd424370671814a862913c99a6e1441588	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/3bfbf5f0a99c991769ec562721285df7ab69240b	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 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