crypto: caam - fix overflow on long hmac keys

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-43330
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 14:16:42 UTC
Updated	2026-05-11 08:16:09 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: crypto: caam - fix overflow on long hmac keys When a key

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000180000 probability, percentile 0.049330000 (date 2026-05-10)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 199354d7fb6eaa2cc5bb650af0bca624baffee35 31022cfde5235c45fa765f0aabeff5f0652852f2 git
CNA	Linux	Linux	affected 199354d7fb6eaa2cc5bb650af0bca624baffee35 c2fb4984fe09fc176fe4c12d5e3edf626df6511d git
CNA	Linux	Linux	affected 199354d7fb6eaa2cc5bb650af0bca624baffee35 aa545df011338df13f0833fc1fabcb15c0521959 git
CNA	Linux	Linux	affected 199354d7fb6eaa2cc5bb650af0bca624baffee35 cebc5ebd958346195b77f42d0cd5141b4e448fae git
CNA	Linux	Linux	affected 199354d7fb6eaa2cc5bb650af0bca624baffee35 80688afb9c35b3934ce2d6be9973758915e2e0ef git
CNA	Linux	Linux	affected 6.3
CNA	Linux	Linux	unaffected 6.3 semver
CNA	Linux	Linux	unaffected 6.6.134 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.81 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/c2fb4984fe09fc176fe4c12d5e3edf626df6511d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/aa545df011338df13f0833fc1fabcb15c0521959	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/80688afb9c35b3934ce2d6be9973758915e2e0ef	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/31022cfde5235c45fa765f0aabeff5f0652852f2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/cebc5ebd958346195b77f42d0cd5141b4e448fae	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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