lib/crypto: chacha: Zeroize permuted_state before it leaves scope

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

Summary

CVE	CVE-2026-43336
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 14:16:43 UTC
Updated	2026-05-11 08:16:10 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: lib/crypto: chacha: Zeroize permuted_state before it leaves

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:H/I:N/A:N

EPSS: 0.000240000 probability, percentile 0.070400000 (date 2026-05-10)

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:H/I:N/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected c08d0e647305c3f8f640010a56c9e4bafb9488d3 e90ee961af515a484f091678ce58a4c3f7b73b02 git
CNA	Linux	Linux	affected c08d0e647305c3f8f640010a56c9e4bafb9488d3 b416a4245f04a450c67a13e6d96056c37c5b33fe git
CNA	Linux	Linux	affected c08d0e647305c3f8f640010a56c9e4bafb9488d3 bd62d9b44464a6c20a34a74068e7a784d0afa04a git
CNA	Linux	Linux	affected c08d0e647305c3f8f640010a56c9e4bafb9488d3 066c760acead1fb743bae294dbd89f479ae43b9b git
CNA	Linux	Linux	affected c08d0e647305c3f8f640010a56c9e4bafb9488d3 1d761e5a7340c46479fb2399598f331e4fe2c633 git
CNA	Linux	Linux	affected c08d0e647305c3f8f640010a56c9e4bafb9488d3 1933249263c3a98df79992f61a566476e4163bcc git
CNA	Linux	Linux	affected c08d0e647305c3f8f640010a56c9e4bafb9488d3 91999af43ca2125e3b2c18fcfc02912ada02efc3 git
CNA	Linux	Linux	affected c08d0e647305c3f8f640010a56c9e4bafb9488d3 e5046823f8fa3677341b541a25af2fcb99a5b1e0 git
CNA	Linux	Linux	affected 4.2
CNA	Linux	Linux	unaffected 4.2 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.169 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.135 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.82 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/e5046823f8fa3677341b541a25af2fcb99a5b1e0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e90ee961af515a484f091678ce58a4c3f7b73b02	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1d761e5a7340c46479fb2399598f331e4fe2c633	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/bd62d9b44464a6c20a34a74068e7a784d0afa04a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b416a4245f04a450c67a13e6d96056c37c5b33fe	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/91999af43ca2125e3b2c18fcfc02912ada02efc3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1933249263c3a98df79992f61a566476e4163bcc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/066c760acead1fb743bae294dbd89f479ae43b9b	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 registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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