Vault Vulnerable to Denial-of-Service via Unauthenticated Root Token Generation/Rekey Operations

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

Summary

CVE	CVE-2026-5807
State	PUBLISHED
Assigner	HashiCorp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 05:16:19 UTC
Updated	2026-04-17 15:08:25 UTC
Description	Vault is vulnerable to a denial-of-service condition where an unauthenticated attacker can repeatedly initiate or cancel root t

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security@hashicorp.com

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

EPSS: 0.000140000 probability, percentile 0.024980000 (date 2026-04-20)

Problem Types: CWE-770 | CWE-770 CWE-770: Allocation of Resources Without Limits or Throttling

Version	Source	Type	Score	Severity	Vector
3.1	security@hashicorp.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	HashiCorp	Vault	affected 2.0.0 semver	64 bit, 32 bit, x86, ARM, MacOS, Windows, Linux
CNA	HashiCorp	Vault Enterprise	affected 2.0.0. semver	64 bit, 32 bit, x86, ARM, MacOS, Windows, Linux

References

Reference	Source	Link
discuss.hashicorp.com/t/hcsec-2026-08-vault-vulnerable-to-denial-of-service-via-una...	security@hashicorp.com	discuss.hashicorp.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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