Vault Token Leaked to Backends via Authorization: Bearer Passthrough Header

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

Summary

CVE	CVE-2026-4525
State	PUBLISHED
Assigner	HashiCorp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 04:16:09 UTC
Updated	2026-04-17 15:08:25 UTC
Description	If a Vault auth mount is configured to pass through the "Authorization" header, and the "Authorization" header is used to au

Risk And Classification

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

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

EPSS: 0.000150000 probability, percentile 0.029130000 (date 2026-04-20)

Problem Types: CWE-201 | CWE-201 CWE-201: Insertion of Sensitive Information Into Sent Data

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	HashiCorp	Vault	affected 0.11.2 2.0.0 semver	64 bit, 32 bit, x86, ARM, MacOS, Windows, Linux
CNA	HashiCorp	Vault Enterprise	affected 0.11.2 2.0.0 semver	64 bit, 32 bit, x86, ARM, MacOS, Windows, Linux

References

Reference	Source	Link
discuss.hashicorp.com/t/hcsec-2026-07-vault-may-expose-tokens-to-auth-plugins-due-t...	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.