HCSEC-2026-07 - Vault May Expose Tokens to Auth Plugins Due to Incorrect Header Sanitization

security-vault

---

mark.collao 1 April 17, 2026, 2:58am

Bulletin ID: HCSEC-2026-07
Affected Products / Versions:
Vault Community Edition from 0.11.2 up to 1.21.4, fixed in 2.0.0.
Vault Enterprise from 0.11.2 up to 1.21.4, 1.20.9, and 1.19.15; fixed in 2.0.0, 1.21.5, 1.20.10, and 1.19.16.
Publication Date: April 16th, 2026

Summary
If a Vault auth mount is configured to pass through the “Authorization” header, and the “Authorization” header is used to authenticate to Vault, Vault forwarded the Vault token to the auth plugin backend. This issue, CVE-2026-4525, is fixed in Vault Community Edition 2.0.0 and Vault Enterprise 2.0.0, 1.21.5, 1.20.10, and 1.19.16.

Background
Vault auth methods allow operators to configure which headers to pass through to a plugin using **passthough_request_headers**.

Details
Due to a flaw in the request processing logic, Vault did not strip the Vault token from the forwarded header. Vault will now strip the Vault token used in the request to the auth plugin backends when making a request, even if the auth method is configured to pass through the header.

Remediation
Customers should evaluate the risk associated with this issue and consider upgrading to Vault Community Edition 2.0.0 or Vault Enterprise 2.0.0, 1.21.5, 1.20.10, and 1.19.16. Please refer to **Upgrading Vault** for general guidance.

Acknowledgement
This issue was identified and reported by Oleh Konko of 1seal.

*We deeply appreciate any effort to coordinate disclosure of security vulnerabilities. For information about security at HashiCorp and the reporting of security vulnerabilities, please see **https://hashicorp.com/security**.*

1 Like

Related topics

Topic	Replies	Activity
HCSEC-2024-18 - Vault Leaks Client Token and Token Accessor in Audit Devices security-vault	0	August 31, 2024
HCSEC-2022-08 - Vault Enterprise’s Tokenization Transform Configuration Endpoint May Expose Transform Key security-vault	0	March 4, 2022
HCSEC-2026-06 - Vault Vulnerable to Server-Side Request Forgery in ACME Challenge Validation via Attacker-Controlled DNS security-vault	0	April 17, 2026
When is the next release for github.com/vault/api?	1	August 7, 2025
Vault 1.17.2, 1.16.6, and 1.15.12 released! vault-release-ce-ent	0	July 10, 2024