HCSEC-2026-05 - Vault KVv2 Metadata and Secret Deletion Policy Bypass Denial-of-Service

security-vault

---

mark.collao 1 April 17, 2026, 2:39am

Bulletin ID: HCSEC-2026-05
Affected Products / Versions:
Vault Community Edition 0.10 up to 1.21.4, fixed in 2.0.0
Vault Enterprise 0.10 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
An authenticated user with access to a kvv2 path through a policy containing a glob may be able to delete secrets they were not authorized to read or write, resulting in denial-of-service. This vulnerability did not allow a malicious user to delete secrets across namespaces, nor read any secret data. This vulnerability, CVE-2026-3605, 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's **kv (Key Value) v2 secrets engine** stores and versions arbitrary static secrets. **The kvv2 API** provides data and metadata paths.

Details
Due to the separate request flows for metadata and data, read access to secret data was not possible. Vault will now enforce the use of canonical paths by clients when requesting access to kvv2 data and metadata.

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 independently identified and reported by Chung Kim from OneMount Group, as well as Andy RUSSON et Gabriel DEPARTOUT from Almond.eu, sponsored the ANSSI (French Cybersecurity Agency) open-source security audit program.

*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**.*

Related topics

Topic	Replies	Activity
HCSEC-2020-03 - Vault Enterprise's Dynamic Secrets May Persist After Namespace Deletion security-vault	0	November 25, 2020
HCSEC-2021-33 - Vault's KV Secrets Engine With Integrated Storage Exposed to Authenticated Denial of Service security-vault	0	December 14, 2021
HCSEC-2021-03 - Vault API Endpoint Allowed Enumeration of Secrets Engine Mount Paths Without Authentication security-vault	0	January 29, 2021
HCSEC-2025-09 - Vault May Expose Sensitive Information in Error Logs When Processing Malformed Data With the KV v2 Plugin security-vault	0	May 2, 2025
Vault_kv_secret_v2 require access to the metadata/... path even if I'm only updating a secret under data/	1	October 16, 2025