HCSEC-2026-02 - Consul Vulnerable to Arbitrary File Reads Through the Vault Kubernetes Authentication Provider

security-consul

---

dduzgun-security 1 March 11, 2026, 11:07pm

Bulletin ID: HCSEC-2026-02
Affected Products / Versions:
Consul Community Edition up to 1.22.4, fixed in 1.22.5.
Consul Enterprise up to 1.18.20, 1.21.10 and 1.22.4 fixed in 1.18.21, 1.21.11 and 1.22.5.

Publication Date: March 11, 2026

Summary
HashiCorp Consul and Consul Enterprise 1.18.20 up to 1.21.10 and 1.22.4 are vulnerable to arbitrary file read when configured with Kubernetes authentication. This vulnerability, CVE-2026-2808, is fixed in Consul 1.18.21, 1.21.11 and 1.22.5.

Background
The **Consul kubernetes auth method** type allows for a Kubernetes service account token to be used to authenticate to Consul within a Kubernetes pod.

Details
When the Connect CA provider uses Vault with Kubernetes authentication method, it reads a ServiceAccount token from a file path specified by the configuration parameter. A privileged attacker with the operator write permission can set the token_path to any file on the Consul server node. The file contents are then returned as data and sent to Vault as part of the Kubernetes authentication request. This leads to potential arbitrary file read and exfiltration from the Consul server host and can result in sensitive data leak. Consul will now only read Kubernetes service accounts tokens from a **defined subset of directories**.

Remediation
Customers using Consul's should evaluate the risk associated with this issue and consider upgrading to Consul Community Edition 1.22.5 or Consul Enterprise 1.18.21, 1.21.11 and 1.22.5.

See Consul's **Upgrading** documentation for general guidance on this process.

Acknowledgement
This issue was identified by Defang Bo.

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
ANN: Consul 1.8.6, 1.7.10 and 1.6.10 Released	0	November 20, 2020
HCSEC-2020-22 - Consul Operator Read ACL Enables Connect Service Masquerading security-consul	0	November 25, 2020
HCSEC-2021-07 - Consul API KV Endpoint Vulnerable to Cross-Site Scripting security-consul	0	April 19, 2021
HCSEC-2022-19 - Consul Auto-Config JWT Authorization Missing Input Validation security-consul	0	September 21, 2022
Consul 1.6.6 and 1.7.4 Released (security)	1	June 10, 2020