HCSEC-2025-29 - Consul's KV endpoint is vulnerable to denial of service

security-consul

---

dduzgun-security 1 October 28, 2025, 8:18pm

Bulletin ID: HCSEC-2025-29
Affected Products / Versions:
Consul Community Edition up to 1.21.5, fixed in 1.22.0.
Consul Enterprise up to 1.21.5, 1.20.7, 1.19.9 and 1.18.11 fixed in 1.22.0, 1.21.6, 1.20.8 and 1.18.12.

Note: Consul Enterprise 1.19 is no longer part of the Long-Term Support (LTS) versions therefore won't get a fix for this finding. We strongly recommend customers upgrading to a newer version.

Publication Date: October 28, 2025

Summary
Consul and Consul Enterprise's ("Consul") key/value endpoint is vulnerable to denial of service (DoS) due to incorrect Content Length header validation. This vulnerability, CVE-2025-11374, is fixed in Consul Community Edition 1.22.0 and Consul Enterprise 1.22.0, 1.21.6, 1.20.8 and 1.18.12.

Background
Consul's KV endpoint allows customers to access Consul's simple key/value store, useful for storing indexed objects, though its main uses are storing configuration parameters and metadata.

Details
Excluding the Content-Length header in the Consul's KV endpoint allowed an attacker to bypass the content length verification. This vulnerability allowed an attacker to send large payloads, which were copied into the buffer, potentially leading to a denial of service (DoS) or system instability due to memory exhaustion.

Remediation
Customers using Consul's should evaluate the risk associated with this issue and consider upgrading to Consul Community Edition 1.22.0 or Consul Enterprise 1.22.0, 1.21.6, 1.20.8 and 1.18.12.

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

Acknowledgement
This issue was identified by Julien Ahrens from RCE Security (**https://www.rcesecurity.com/**).

*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-2025-28 - Consul's event endpoint is vulnerable to denial of service security-consul	0	October 28, 2025
HCSEC-2021-07 - Consul API KV Endpoint Vulnerable to Cross-Site Scripting security-consul	0	April 19, 2021
HCSEC-2020-14 - Consul DNS and HTTP Cache Abuse Denial of Service security-consul	0	November 25, 2020
HCSEC-2020-02 - Consul’s HTTP/RPC Services Allow Unbounded Resource Usage, Susceptible to Unauthenticated Denial of Service security-consul	0	November 25, 2020
Consul 1.6.3 Released (security)	5	January 31, 2020