April 2, 2024

HashiCorp
101 2nd St #575
San Francisco, CA
94105

To Whom It May Concern:

Leidos completed its conformance review of the -fips builds of the following HashiCorp products (hereafter referred to as the "Product") on April 2, 2024:

- Consul Enterprise builds 1.16.0 and 1.16.1
- Consul Dataplane builds 1.2.0 and 1.2.1
- Consul K8s builds 1.2.0 and 1.2.1
- Consul K8s Control Plane builds 1.2.0 and 1.2.1

Leidos has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic module:

- BoringCrypto (FIPS 140-2 Cert. #4407). This will be referred to as the "Integrated Cryptographic Module" throughout the remainder of this document.

Specifically, when deployed on the following platforms:
- Linux 4.X executing on x86_64 architecture
- Linux 4.X executing on Aarch64 architecture
- Linux 5.X executing on x86_64 architecture
- Linux 5.X executing on Aarch64 architecture

Leidos' review confirmed that the Integrated Cryptographic Module is properly being leveraged for, but not limited to, the following features and use cases and assumptions:

1. The Consul CLI 'keygen' command uses the Integrated Cryptographic Module to generate encryption keys.
2. The Consul CLI 'tls ca create' command uses the Integrated Cryptographic Module to generate CA certificates and key pairs.
3. The Consul CLI 'tls cert create' command uses the Integrated Cryptographic Module to generate TLS certificates and key pairs.
4. The Consul agent uses the Integrated Cryptographic Module to encrypt network traffic in the Gossip Protocol.
    a. Assumption: 'encrypt' configuration parameter must be set in the config file to a 32-byte, base64 encoded key
5. The Consul agent uses the Integrated Cryptographic Module to perform TLS for mutual authentication and encryption of RPC calls between agents.
    a. Assumption: 'verify_outgoing' and 'verify_incoming' options must be set, and the client and server nodes must have an appropriate key pair set using 'cert_file' and 'key_file' configurations
6. The Consul auto-encryption feature uses the Integrated Cryptographic Module to generate TLS certificates, CSRs, and key pairs for clients.
    a. Assumption: 'auto_encrypt {allow_tls = true}' must be set
7. Consul uses the Integrated Cryptographic Module to sign leaf certificates used by Connect proxies.
8. Consul uses the Integrated Cryptographic Module to generate and sign CA certificates and CSRs for the Service Mesh
9. Consul Connect Proxies and Services uses the Integrated Cryptographic Module for TLS connections.

10. Consul Watches use the Integrated Cryptographic Module to establish TLS connections with HTTPS endpoints.
11. The Consul API uses the Integrated Cryptographic Module to establish TLS connections with Consul nodes.
12. Consul JSON Web Token (JWT) Auth Method uses the Integrated Cryptographic Module to parse asymmetric public keys and validate JWT signatures.
13. Consul Cluster Peering uses the Integrated Cryptographic Module to establish TLS connections between Consul clusters.
14. The 'Consul on Kubernetes' 'consul-k8s-control-plane tls-init' command uses the Integrated Cryptographic Module to generate CA and server certificates.
15. The 'Consul on Kubernetes' 'consul-k8s-control-plane gossip-encryption-autogenerate' command uses the Integrated Cryptographic Module to generate Gossip encryption keys.
16. The Consul CLI 'login' command uses the Integrated Cryptographic Module for TLS connection to Kubernetes when using the 'kubernetes' auth method.
17. 'Consul on Kubernetes' uses the Integrated Cryptographic Module for TLS connections to Consul and Kubernetes. The Product will not operate if the Integrated Cryptographic Module is missing or altered.
18. The Product will not operate if the Integrated Cryptographic Module is missing or altered.

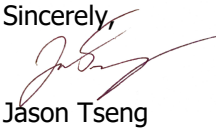
Details of Leidos' review, which consisted of source code review and operational testing, are obtainable by special request.

Please note that for this review, Leidos only examined the Product features referenced above and while the Product may contain other features or functionality, Leidos did not examine these during its review and makes no claims or representations regarding them. Furthermore, the Cryptographic Module Validation Program (CMVP) has not independently reviewed Leidos' analysis, testing, or results.

The intention of this letter is to provide independent opinion that the Product correctly integrates and uses validated cryptographic modules within the scope of claims indicated above. Leidos offers no warranties or guarantees with respect to the above-described compliance review. This letter does not imply a Leidos certification or product endorsement.

Please let us know if you have any questions.

Sincerely,



Jason Tseng
Leidos Cryptographic and Security Testing Laboratory (CSTL) Lab Director