June 28, 2022

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

To Whom It May Concern:

Leidos completed its conformance review of the HashiCorp Vault **1.10.4-ent (with or without FIPS Enabled)** build (the "Product") on June 28, 2022; and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic module:

1. NITROXIII CNN35XX-NFBE HSM Family (FIPS 140-2 Cert. #4218). This will be referred to as the "Integrated Cryptographic Module" throughout the remainder of this document.

Specifically, under the following assumptions:

1. The Integrated Cryptographic Module is initialized in a manner that is compliant with its Security Policy.

2. The Product is configured to use the Integrated Cryptographic Module via a 'seal' block specifying a seal type of 'pkcs11' in the Product's configuration file.

Leidos' review confirmed that:

1. All cryptographic operations for encryption, decryption, message authentication code generation, message authentication code verification, and cryptographic key generation used for Managed Keys, Seal Wrapping and Unwrapping are offloaded to the Integrated Cryptographic Module. Secrets protected by the Integrated Cryptographic Module are protected by encryption and message authentication codes in a fashion that is compliant to the FIPS 140-2 guidance for both Key Storage (as per FIPS 140-2 IG 7.16) and Key Transport (as per FIPS 140-2 IG D.9).

2. Secrets and paths designated as "Always Seal Wrap" in the Product are protected using the Integrated Cryptographic Module for seal wrapping. The secrets and paths designated as "Always Seal Wrap" in the Product include the following:

    a. The Keyring (core/keyring)
    b. The Keyring Update Entry Path (All files under core/upgrade/)
    c. The Master Key (core/master)
    d. The Replication Token Generation Key (core/wrapping/jwtkey)
    e. Local CA Information (All files under core/leader/)
    f. Cluster Information (core/cluster/local/info)
    g. Replicated Cluster Information Path (All files under core/cluster/replicated/)
    h. Replicated Cluster Information Path for Disaster Recovery (All files under core/cluster/replicated-dr/)
    i. Multi-Factor Authentication TOTP Keys Path (All files under sys/mfa/totpkeys/)
    j. The Disaster Recovery Operation Token (core/dr-operation-token)
    k. The Key Encryption Key for the Shamir Master Key (core/shamir-kek)

3. When a backend is configured with seal wrapping enabled with the Product, all Keys and Critical Security Parameters written to the backend are protected using the Integrated Cryptographic Module for seal wrapping. The Keys and Critical Security Parameters covered by seal wrapping include:

a. The CA Key (config/ca_bundle) used in the PKI secret backend
b. The Keys (policy/) and Key Archives (archive/) used in the Transit secret backend
c. The CA Key (ca_private_key, config/ca_private_key) and generated SSH RSA Keys (keys/*) used in the SSH secret backend
d. The Keys (key/) used in the TOTP secret backend
e. All Storage Entries used in the KV backend
f. AWS Access Keys (config/client) used in the AWS authentication backend
g. LDAP Credentials (config) used in the LDAP authentication backend
h. Okta Credentials (config) used in the Okta authentication backend
i. RADIUS Credentials (config) used in the RADIUS authentication backend
j. AWS Root Credentials (config/root) used in the AWS secret backend
k. Cassandra Credentials (config/connection) used in the Cassandra secret backend
l. Consul Credentials (config/access) used in the Consul secret backend
m. Database Credentials (config/ and static-role/) used in the plugin-based Database secret backend
n. MongoDB Credentials (config/connection) used in the MongoDB secret backend
o. MSSQL Credentials (config/connection) used in the MSSQL secret backend
p. MySQL Credentials (config/connection) used in the MySQL secret backend
q. PostgreSQL Credentials (config/connection) used in the PostgreSQL secret backend
r. RabbitMQ Credentials (config/connection) used in the RabbitMQ secret backend
s. Nomad Credentials (config/access) used in the Nomad secret backend

4. 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