ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Venafi Trust Protection Platform

---

Maintenance Update of Venafi Trust Protection Platform

Maintenance Report Number: CCEVS-VR-VID10800-2018

Date of Activity: 27 August 2018

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- Venafi Trust Protection Platform Impact Analysis Report for Common Criteria Assurance Maintenance, version 18.1
- Protection Profile for Application Software, version 1.2, dated 22 April 2016 [SWAPP]
- Extended Package for Secure Shell, version 1.0, dated 19 February 2016 [SSHEP]

Documentation reported as being updated:

- Venafi Trust Protection Platform 18.1 Security Target, Version 1.2, August 2018;
- Venafi Trust Protection Platform 18.1 Common Criteria Guidance, Version 1.1, June 27, 2018

Assurance Continuity Maintenance Report:

Venafi submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 20 July 30, 2018. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The IAR identified changes to the TOE including several software security updates and non-security relevant feature updates. The platform has had four version updates since the original product was certified. The security updates ensure that the software maintenance is current, including bugs fixes and security updates have been applied. No hardware changes were reported.

The evaluation evidence consisted of the Security Target, Impact Analysis Report (IAR), and User Guidance. The Security Target was revised to introduce the updated platform version number. The User Guide was similarly revised to identify current platform version. The IAR was new.

The evaluation was performed against the collaborative Protection Profile for Application Software, version 1.2, and the Extended Package for Secure Shell, version 1.0. The ST referenced validated FIPS certificates. No changes were made in the processor, and the bug fixes had no effect on cryptographic processing, so no modifications were required in any of the valid NIST certificates.

Changes to TOE:

Fifty-Eight Software changes and bug fixes were identified and claimed to be non-security relevant system updates across four platform version updates. A complete listing of the software changes, per version, was supplied in the IAR. The changes were either associated with non-security relevant commands and configuration or for functions/components not claimed in the original evaluation.

A detailed description of each change and the associated impact and rational was provided for all the changes in each platform version. The rational provided supporting evidence to ensure that the changes were not TOE security relevant and outside the scope of the TOE security boundary.

Changes to Evaluation Documents:

- ST: Updated to indicate current Venafi Trust Protection Platform software version.
- AGD: Updated to indicate current Venafi Trust Protection Platform software version

Regression Testing:

Although no changes were made to the security functionality of the TOE, vulnerability testing, functional regression testing and unit testing was performed against each release and software build. The regression testing included automation testing and manual test execution by the Quality Assurance Team.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor or irrelevant. All bug fixes were for non-security-relevant functions and did not affect any TOE Security Functions.

The vendor reported that the updated TOE modules did undergo regression testing for each new platform release.

The CCTL also reported that there were no known vulnerabilities associated with any of the product releases. Public domain vulnerability searches were performed against vulnerability databases to ensure the TOE was not vulnerable to known attacks.

Therefore, CCEVS agrees that the original assurance is maintained for the product.