ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
Venafi Trust Protection Platform, V21.1

Maintenance Update of Venafi Trust Protection Platform, V21.1

Maintenance Report Number: CCEVS-VR-VID11024-2022

Date of Activity: 31 January 2022

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 Update from Version 20.1 to Version 21.1, v1.1, 21 January 2022.
- Protection Profile for Application Software, version 1.3, dated 01 March 2019 [SWAPP].
- Extended Package for Secure Shell, version 1.0, dated 19 February 2016 [SSHEP].

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: Venafi Trust Protection Platform Security Target, Version 4.0	**Maintained Security Target:** Venafi Trust Protection Platform Security Target, Version 4.1 Changes in the maintained ST are: • Version number of TOE changed from 20.1 to 21.1 • Version number of document changed to 4.1.

Common Criteria Compliance Guide: Venafi Trust Protection Platform 20.1 Common Criteria Guidance, v1.2	**Maintained Common Criteria Compliance Guide:** Venafi Trust Protection Platform 21.1 Common Criteria Guidance, v1.3 Changes in the maintained Guidance are: • Version number of TOE changed from 20.1 to 21.1 • Version number of document changed to 1.3

Assurance Continuity Maintenance Report:

Venafi, Inc., submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 21 January 2022. 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 evaluation evidence consists of the Security Target, the CC Compliance Guide, and the Impact Analysis Report (IAR). The ST and guide document were updated, the IAR was new.

Changes to TOE:

For this Assurance Continuity, the version number of TOE changed from 20.1 to 21.1. The version change from 20 to 21 represents the year of release rather than being tied to a major or minor nomenclature. The following paragraphs list the minor software changes and fixes made to the TOE during the maintenance cycle.

Software Changes

The developer reported the new features/changes to the product located in the tables below:

Added support for Azure SQL Managed instances. • **Impact: Minor** • **Rationale: The feature is regarding to interaction with a 3rd party device which is not part of the TOE or the claimed security functionality**
Added support for GPG and .NET environments. • **Impact: Minor** • **Rationale: The feature is regarding to interaction with a 3rd party device which is not part of the TOE or the claimed security functionality**
Added support for google cloud DB. • **Impact: Minor** • **Rationale: The feature is regarding to interaction with a 3rd party device which is not part of the TOE or the claimed security functionality**
Added support for 3rd party identity management applications • **Impact: Minor** • **Rationale: The feature is regarding to interaction with a 3rd party device which is not part of the TOE or the claimed security functionality**
Interface improvements for SAML interactions. • **Impact: Minor** • **Rationale: The feature is regarding to interaction with a 3rd party device which is not part of the TOE or the claimed security functionality**
Continued improvement in user interface. • **Impact: Minor** • **Rationale: This is a usability feature that does not affect any of the security claims within the evaluation**
Added an option in the Venafi Conguration Console to create a newAnswer File, which allows you to generate an answer file for additional installations • **Impact: Minor** • **Rationale: This is a usability feature that does not affect any of the security claims within the evaluation**
Administrators can now modify the default menu settings. • **Impact: Minor** • **Rationale: This is a usability feature that does not affect any of the security claims within the evaluation**
Improved interface accessibility, making the interface useable for people of all abilities. • **Impact: Minor** • **Rationale: This is a usability feature that does not affect any of the security claims within the evaluation**

Software Fixes

The following list of software fixes have been addressed as of version 21.1 of the TOE. These have been included to verify that the TOE maintenance cycle is maintained to ensure all bugs and code fixes are addressed during the life cycle. Numbers starting with a hash symbol (#) indicate internal Venafi tracking numbers. Numbers starting with the at symbol (@) indicate the incident number issued by support.venafi.com.

HSM Errors with an nCipher device when an Admin Card was in a slot. #66708

- **Impact: Minor**
- **Rationale: This is bug fix that does not change security functionality/affect any SFRs.**

Notifications were not sent when condition is set on data column. #48026

- **Impact: Minor**
- **Rationale: This is bug fix that does not change security functionality/affect any SFRs.**

When an administrator customized the product menu for "Everyone else" and had not customized their own menu, the "Everyone Else" settings were also applied to the admin's menu. #65051

- **Impact: Minor**
- **Rationale: This is bug fix that does not change security functionality/affect any SFRs.**

Changing product landing page was not reflected until user logs out. #65090

- **Impact: Minor**
- **Rationale: This is bug fix that does not change security functionality/affect any SFRs.**

When renewing, the JAMF integration created new certificates instead of merging with the previous certificate (and putting the previous certificate in the historical certificates tab). #64956

- **Impact: Minor**
- **Rationale: This is bug fix that does not change security functionality/affect any SFRs.**

Unable to select extracting PEM certificate content into separate files in Aperture. #66128

- **Impact: Minor**
- **Rationale: This is bug fix that does not change security functionality/affect any SFRs.**

"Index was outside the bounds of the array" error was displayed when some users tried to log into the web console. #65621

- **Impact: Minor**
- **Rationale: This is bug fix that does not change security functionality/affect any SFRs.**

When multiple identities were logged, the VCC Event Viewer does not translate identities to the friendly name. #65140

- **Impact: Minor**

- **Rationale: This is bug fix that does not change security functionality/affect any SFRs.**

Changes to Evaluation Documents:

ST was modified to reflect changes to version number of TOE changed from 20.1 to 21.1. Also, version number of the document changed to 4.1.

Common Criteria Compliance Guide was modified to reflect the version number of TOE changed from 20.1 to 21.1. Also, version number of the document changed to 1.3.

Regression Testing:

In addition to the vendor performing vulnerability testing, functional regression testing and unit testing is also performed against each release and/or software build to ensure the TOE functionality is maintained and that the source code is fit for use. This functional testing included verification that any newly introduced feature does not affect the security functionality previously tested and verified. The regression testing performed against the TOE includes partial automation testing as well as manual test execution by the Quality Assurance Team within Venafi. This testing ensures that the functionality claimed within the Security Target has not been impacted by any software changes made to the product between releases. The unit testing is performed against each software build to ensure that the source code used in each release is fit for use and performing in the expected manner

For instances when security related bugs were identified, the vendor performed specific testing on the updates to ensure that the identified behavior is no longer present within the TOE and the TOE operates as expected. After this is successfully confirmed, the testing is incorporated into the regular regression testing and rerun until the TOE software is released.

NIST CAVP Certificates:

The TOE relies on the platform for cryptography.

Vulnerability Analysis:

Public domain searches were performed using the publicly available vulnerability databases. Searches were made for potential vulnerabilities in the TOE using the websites listed below. The sources of the publicly available information are provided below.

- http://nvd.nist.gov
- http://www.us-cert.gov
- http://www.securityfocus.com

The evaluator performed the public domain vulnerability searches using the following key words.

- Venafi
- Trust Platform
- JSON.Net
- PDFSharp
- MigraDocm
- HTMLAgility Pack
- MS Anti-Cross Site Scripting Library
- IronPython
- jQuery v3.4.1
- Moment JS v2.24.0
- Backbone JS v1.4.0
- Twitter bootstrap Apache v2
- Underscore
- Boost
- Beast
- JSON11
- Base64
- Cxxopts
- Chaos.NaCI

Selected search key words based upon the following criteria:

- The vendor name was searched,
- The software running on the TOE devices were searched. Further, the version the TOE software in evaluation was searched,
- The name of the hardware devices within the TOE,
- The secure protocols supported by the TOE,
- The type of TOE device.

The search was performed on the following dates: 8/31/2021 and 1/10/2022. This spans the time since the last Assurance Maintenance. None of the identified CVEs were related to a Venafi product.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. No functionality, as defined in the SFRs, was impacted, and none of the software updates affected the security functionality or the SFRs identified in the Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.