ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
Venafi Trust Protection Platform, V20.1

Maintenance Update of Venafi Trust Protection Platform, V20.1
Maintenance Report Number: CCEVS-VR-VID11024-2020

Date of Activity: 12 October 2020

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 19.2.6 To Version 20.1, V1.1, 9/30/2020.
- 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 4.0 Changes in the maintained ST are: • Version number of TOE changed from 19.2.6 to 20.1 • Version number of document changed to 4.0.
Common Criteria Compliance Guide: Venafi Trust Protection Platform 20.1 Common Criteria Guidance, v1.2	**Maintained Common Criteria Compliance Guide:** Venafi Trust Protection Platform 20.1 Common Criteria Guidance, v1.2 Changes in the maintained Guidance are: • Version number of TOE changed from 19.2.6 to 20.1

	• Version number of document changed to 1.2.

Assurance Continuity Maintenance Report:

Venafi, Inc., submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 8/18/2020. 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, IAR was new.

The evaluation was done against the:

- 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].

The TOE relies on the platform for cryptographic services.

Changes to TOE:

For this Assurance Continuity, the version number of TOE changed from 19.2.6 to 20.1. The following paragraphs list the minor software updates and fixes made to the TOE during the maintenance cycle.

MS SQL Server 2017 database can now be used. Rationale: The feature interacts with a 3rd party device which is not part of the TOE or the claimed security functionality

A master administrator can now view the owner of custom reports and can reassign a custom report to a new owner. Rationale: Operations with reports do not affect any of the security claims within the evaluation

An Enhancement was made to help Customer Support more effectively assist customers needing help troubleshooting homegrown Adaptable scripts. Rationale: This is a troubleshooting usability feature that does not affect any of the security claims within the evaluation

The Trust Protection Platform can now be configured to authenticate to an SCIM server when setting up the CyberArk connector in the Venafi Configuration Console (VCC). Rationale: The feature is regarding to interaction with a 3rd party device which is not part of the TOE or the claimed security functionality

The rationale for the following software changes is that they are usability features that does not affect any of the security claims within the evaluation

1. Previous versions limited only 1,000 characters in the command line injection. Due to improvements to how Workflow configurations are stored in the database, the is no longer a storage limit on the number of characters for command injection purposes.
2. The certificate inventory in Aperture now includes an additional filter, allowing filtering based on CA Template.
3. If a policy requires Custom Fields, requests must include the Custom Field value.
4. Instead of command line flags for Discovery/Import, a JSON input file with the Scanafi provider or standalone mode is used.
5. The Log and Workflow Swagger modules allow you to try the Web SDK Log and Workflow interfaces in your test environment.
6. Roles associated with the product are now included in the Entitlement Report.
7. Trust Protection platform now updates information dynamically, instead of manually selecting controllers or global catalogs.
8. When creating custom reports in Trust Protection Platform, a new option lets you skip sending the report if the report data is empty.
9. Increased contrast for widget buttons, screen reader enhancements for menus and clickable elements, focus improvements for clickable elements, image titles, and alt text.
10. To delete network discovery jobs, DELETE Discovery/{guid} can now be used.
11. The local Identity group can now contain members from any Identity Provider.
12. Active Directory, LDAP, or local members can now be added to a local Identity group.
13. Member entries will now remain in the Identity Provider When the local Identity group is deleted.

The following bug fixes were judged to have a minor impact. They either do not impact functionality claims or are below the visibility of the SFR testing.

1. Previously, when there were many applications on a device (common with load balancers), both onboard and network validation could delay certificate provisioning (installation).
2. Locking ECC policy value correctly greys out the corresponding choices on policy subfolders.
3. Notification emails are not sent when the target user email contains a comma.
4. Aperture now displays both credentials when editing a certificate installation for Adaptable Applications.
5. You can now successfully provision when using OpenSSL 1.1.1 and with or without remote key generation (which had previously worked only without remote key generation).
6. Provisioning ACM-issued certificates to ALB/ELB/CF when CA templates are assigned by policy now works as expected.
7. When the target bundle does not exist, provisioning a trust store to an F5 device now functions as expected.
8. The Custom Report CSV format now contains the expected Device and Host Address.
9. When you validate a CA template using an invalid credential for Symantec MPKI, the "Object Reference Not Set" error no longer occurs.

10. Effective Revocation Date for Microsoft CA certificate now correctly matches Revocation Date. CAPI no longer fails onboard validation if hostname set and SNI are not enabled for binding.
11. F5 onboard discovery now finds certificates with no extension.
12. AppCAPI.lsc now references the correct parameter for error message.
13. Disabled attributes no longer being manipulated when saving a project.
14. Correct number of certificates now shown on all widgets on the User and Client Device dashboard.
15. User Agent no longer ignores the "Archived" flag when checking if the certificate is already present in CAPI before provisioning.
16. Different Windows versions are no longer reporting different User Agent headers, thereby allowing the VEDSCEP logic to detect Windows NDES clients.
17. Certificate Grid Revocation filter in WebAdmin now functions correctly with “ != “ (NOT operator).
18. Discovery Zones is no longer stuck in Pending Execution state with multiple Management Servers.
19. Active Directory (AD) wizard can’t complete if domains unreachable.
20. Incorrect password caused Active Directory (AD) wizard to finish. Wizard had to be restarted.
21. Enumeration of installed policy in Aperture is slow when adding a new installation to a certificate.
22. Unable to adjust frequency of recovery to improve performance.
23. CertificateRepair.lsc is not included in the 19.3 MSI.
24. Global Catalog is removed from summary in Identity wizard if it is not a selected Domain Controller.
25. Custom Report Wizard in Aperture now saves edited columns.
26. Report Started and Completed events are now logged, and marked as Deprecated.
27. SSH Discovery delivery of sshd_config no longer incorrectly logs debug message "No response" when no response is the correct behavior.
28. Users can no longer see keysets if they have either Read OR View (not View AND Read) permissions.
29. Keyset is no longer "In Policy" after removing the keyset object from WebAdmin.
30. Changing passphrase for encrypted PK with .pub part now works properly.
31. Device placement from Network Discovery now adds devices that were previously placed and removed.
32. "SSH Authorized Users Report" export now inputs values into the correct columns.
33. Long URLs no longer break custom reports,
34. Adaptable workflow no longer forces workflows to be evaluated and executed one at a time, resulting in faster performance.
35. There is now a dedicated Aperture event for retiring a certificate,
36. Private Key Vault ID is now restored to Cert Object when you have to reset in WebAdmin or Cancel in Aperture during cert renewal.
37. Approval is completed while approval workflow is at Stage 100 in Aperture.

38. Environment certificate status shows “Out of Sync.”
39. Results are able to be exported from Applications View Tab with 1000 or more apps.
40. Locked adaptable application credential not enforced by policy.
41. certbot no longer throws "Invalid key authorization" error when communicating with an ACME server.
42. Certificate Status for Revocation is not updating when revocation has taken place.
43. A renewed certificate name (CN) differed between the API call and the name from the CA.
44. GET Certificates and HEAD Certificates can now return multiple Management Types in the same API call.
45. Long URLs no longer break custom reports,
46. Adaptable workflow no longer forces workflows to be evaluated and executed one at a time, resulting in faster performance.

Changes to Evaluation Documents:

ST was modified to reflect changes to version number of TOE changed from 19.2.6 to 20.1. Also, version number of the document changed to 4.0.

Common Criteria Compliance Guide was modified to reflect the version number of TOE changed from 19.2.6 to 20.1. Also, version number of the document changed to 1.2.

Regression Testing:

Functional regression testing was performed against this maintenance release to ensure the TOE functionality is maintained. 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.

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 databases searched were:

- 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. The search was performed on August 6, 2020.

- 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

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.