ASSURANCE CONTINUITY MAINTENANCE REPORT FOR CertAgent v7.0 patch level 9

Maintenance Update of CertAgent v7.0 patch level 9

Maintenance Report Number: CCEVS-VR-VID11180-2022

Date of Activity: April 21, 2022

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008.
- CertAgent Impact Analysis Report for Common Criteria Assurance Maintenance Update from Version 7.0 patch level 9.0 to Version 7.0 patch level 9.6, v1.0.3, 8 April, 2022.
- Protection Profile for Certification Authorities, version 2.1 [PP_CA_V2.1]

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: • CertAgent Security Target for Common Criteria Evaluation, version 4.2.9, July 27, 2021	**Maintained Security Target:** • CertAgent Security Target for Common Criteria Evaluation, version 4.3.2, 8 April 2022 Changes in the maintained ST are: • Version number of TOE changed from • Version 7.0 patch level 9.0 to Version 7.0 patch level 9.6 • Updated the TOE documentation references

Common Criteria Guidance Documentation	Maintained Common Criteria Guidance documentation:
• CertAgent Guidance for Common Criteria Evaluation, version 2.6.3, July 27, 2021 • CertAgent Installation, Configuration and Management Guide, version 7.0, September 15, 2020 • CertAgent Administrator Guide, version 7.0, September 15, 2020 • CertAgent Certificate Authority Guide, version 7.0, September 15, 2020 • CertAgent Public Site Guide, version 7.0, September 15, 2020 • CertAgent Release Notes, version 7.0.9, January 22, 2021	• CertAgent Guidance for Common Criteria Evaluation, version 2.7.1, April 7, 2022 • CertAgent Installation, Configuration and Management Guide, version 7.0, April 6, 2022 • CertAgent Administrator Guide, version 7.0, April 4, 2022 • CertAgent Certificate Authority Guide, version 7.0, April 4, 2022 • CertAgent Public Site Guide, version 7.0, April 4, 2022 • CertAgent Release Notes, version 7.0.9.6, April 4, 2022 Changes in the maintained Guidance are: • Version 7.0 patch level 9.0 to Version 7.0 patch level 9.6 • Version of Apache Tomcat updated to 8.5.73 from 8.5.57 • Version number of document changed to 2.7.1. • All the changes documented in this report corresponding to the updates to the TOE.

Assurance Continuity Maintenance Report:

Information Security Corporation, submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 11 April 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 guidance documentation were updated, the IAR was new.

Changes to TOE:

For this Assurance Continuity, the version number of TOE changed from Version 7.0 patch level 9.0 to Version 7.0 patch level 9.6. 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 an option to accept non-critical basicConstraints and keyUsage extensions in intermediate CA certificates in path validation • **Impact: Minor** • **Rationale: The feature allows customers to transition from an existing, non-compliant, PKI while enforcing other path validation requirements. Use of this feature is not allowed in the evaluated configuration. The option that places the TOE in the evaluated configuration remains enabled in the NIAP mode as documented in the common criteria guidance and the TOE functionality does not change from the validated TOE security functionality when the option to require critical basicConstraints and keyUsage extensions in intermediate CA certificates is enabled.**
Added a new password-based EST RA role to act as a registration authority to enroll certificates for subscribers via EST using basic authentication • **Impact: Minor** • **Rationale: The feature impacts FIA_ESTS_EXT.1.3. There are no assurance activities associated with this change and only users with valid EST usernames and passwords can enroll a certificate via EST using basic authentication. This new EST RA option is disabled in the evaluated configuration and therefore does not impact the evaluated configuration.**
Added an option to manage EST users via RA Management Interface (RAMI) • **Impact: Minor** • **Rationale: This is a usability feature that which affects the security claims within the evaluation. However, this feature is not used in the evaluated configuration. RAMI management of EST users is disabled in NIAP compliant TOE which is the same as the RAMI setting in the validated TOE**
Apache Tomcat has been updated from version 8.5.57 to version 8.5.73 to address published vulnerabilities and defects. • **Impact: Minor** • **Rationale: The update was performed to address the vulnerabilities associated with the version of the software in the product**
The Apache Log4j 2 library has been updated from version 2.13.3 to version 2.17.1 • **Impact: Minor** • **Rationale: The update was performed to address the vulnerabilities associated with the version of the software in the product**
Google gson library has been updated from version 2.8.6 to version 2.8.9. • **Impact: Minor** • **Rationale: The update was performed to address the vulnerabilities associated with the version of the software in the product**
Updated Linux installation script to support Ubuntu

• **Impact: Minor** • **Rationale: This is a usability feature that does not affect any of the security claims within the evaluation. The vendor is not claiming Ubuntu to be equivalent to the validated platforms or that the TOE can be installed on Ubuntu in the evaluated configuration.**
Updated EST User Self-Service Page • **Impact: Minor** • **Rationale: This is a usability feature that does not affect any of the security claims within the evaluation. This feature allows for searching users by type instead of displaying users in two sections.**
Added an evaluation option to the installer • **Impact: Minor** • **Rationale: This is a usability feature that does not affect any of the security claims within the evaluation. The evaluation copy is the same as the activated copy except a red banner with "Evaluation Copy" will appear on the top of all web pages and "Evaluation Copy" will appear in the About page.**
Updated License Agreement • **Impact: Minor** • **Rationale: This is an update that does not affect any of the security claims within the evaluation. This change provides clarity to the agreement terms between the vendor and their customer.**

Software Fixes

The following list of software fixes have been addressed as of Version 7.0 patch level 9.6 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.

Corrected two rare crashes when signing objects • **Impact: Minor** • **Rationale: This is a bug fix that impacts FCS_COP.1(2) and FCS_COP.1(1). However, it is an alteration to the processing logic to avoid the crash and has no relation to the actual cryptographic operation or the resulting values from the cryptographic operation.**
Credentials, Certificate Issuance, Advanced Certificate Request pages are now displayed properly in Internet Explorer • **Impact: Minor** • **Rationale: This is bug fix that does not change security functionality/affect any SFRs.**
Special characters are now escaped properly in the HSQLDB script and Tomcat configuration file • **Impact: Minor** • **Rationale: This is bug fix that does not change security functionality/affect any SFRs.**

The TOE no longer shuts down after updating the EST user configuration 20 times

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

Changes to Evaluation Documents:

The AGD document named "CertAgent Guidance for Common Criteria Evaluation" has been updated to version 2.7.1, April 7, 2022.

The Security Target document named "CertAgent Security Target for Common Criteria Evaluation" has been updated to version 4.3.2, April 8, 2022.

Regression Testing:

In addition to the vendor performing vulnerability analysis, functional regression testing was also performed against the updated TOE 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. This testing ensured that the functionality claimed within the Security Target has not been impacted by any software changes made to the product between releases.

For instances when security related bugs or general defects 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.

NIST CAVP Certificates:

No changes to the CAVP certificates from the previously evaluated version of the TOE.

Vulnerability Analysis:

On April 8, 2022 ISC performed a vulnerability assessment on the libraries used by the validated and changed TOE using the following resources:

- National vulnerability database:
  https://nvd.nist.gov/vuln/search
- Apache Tomcat 8.x vulnerabilities:
  https://tomcat.apache.org/security-8.html

- Apache Log4j Security Vulnerabilities:

  https://logging.apache.org/log4j/2.x/security.html
- snky open source vulnerability database:

  https://security.snyk.io/
- Google gson change log:

  https://github.com/google/gson/blob/master/CHANGELOG.md

The following search terms were used:

- Apache Tomcat 8.5
- Apache Log4j2
- Gson
- Acalashim
- CDK
- jquery 3.5.1
- jquery 3.5
- jqueryui 1.12.1
- jqueryui

Vulnerability analysis included search of vulnerabilities applicable to the TOE and all the third-party software included as part of the TOE. The issues found were either for those where fixes have been applied in the updated TOE, or were related to other products, and not applicable to the TOE. Additionally, the validation team noted that the list of search terms did not include the name of the product as one of the key words and performed an independent search for vulnerabilities in the sources listed above using “CertAgent” as the search criteria. The search did not result in any applicable entries.

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.