ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Information Security Corporation CertAgent

Maintenance Update of Information Security Corporation CertAgent

Maintenance Report Number: CCEVS-VR-VID10815-2019

Date of Activity: 23 August 2019

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- Information Security Corporation CertAgent Impact Analysis Report (IAR) for Software Version 7.0 patch level 7, version 1.0.1, August 22, 2019
- Protection Profile for Certificate Authorities, version 2.1 (PP_CA)

Documentation reported as being updated:

- CertAgent Security Target for Common Criteria Evaluation, version 4.1.3, August 22, 2019
- CertAgent Guidance for Common Criteria Evaluation, version 2.4.0, July 15, 2019
- CertAgent Installation, Configuration and Management Guide, version 7.0, July 9, 2019
- CertAgent Release Notes, version 7.0.7, July 15, 2019
- CertAgent Administrator Guide, version 7.0, July 9, 2019
- CertAgent Certificate Authority Guide, version 7.0, July 9, 2019
- CertAgent Public Site Guide, version 7.0, July 9, 2019

Assurance Continuity Maintenance Report:

Information Security Corporation (ISC) submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 17 July 2019. 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 in three areas: new features, changes and bug fixes. The changes are identified as being limited in scope and are not considered security related. The TOE changes are identified as mostly as being in the areas of usability and maintainability. Additional detail on the changes and issues and are described in the next few sections. The bug fixes are defect corrections to the TOE and are described in the next section. No hardware changes were reported.

The evaluation evidence consisted of the Security Target, Impact Analysis Report (IAR), and Common Criteria Guidance. The Security Target was revised to introduce the update version number, product changes and component updates. The Common Criteria Guidance was similarly revised to identify the updated version and installation features. The IAR was new.

The evaluation was performed against the Protection Profile for Certification Authorities, version 2.1 (PP_CA_V2.1). 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.

New Features:

An optional TOE installer feature has been added to TOE to allow for an automatic configuration of an HTTP port for OCSP, Issuer Certificate and CRL retrieval. The validated TOE requires that the HTTP port be part of the TOE configuration and this no longer is done manually post installation, as was performed in the previous version of the TOE. The original HTTPS URLs are still accessible. This change automates the HTTP port configuration process and results in the same TOE configuration. The updated detailed installation instructions are contained in section three of the CC Guidance document.

The updated installer also now creates a TLS certificate that includes a Subject Alternative Name extension and uses certificate profiles when creating installer created certificates

A detailed description of each change and the associated impact and rationale was provided for all the TOE changes. The rationale provided supporting evidence to ensure that the changes were either not TOE security relevant or considered minor.

Changes to TOE:

Three TOE change were identified. These changes included an update to the version of Apache Tomcat; installation of Java; and a change to DN encoding.

The Apache Tomcat update, from version 8.5.23 to version 8.5.42, addresses published vulnerabilities in the server. A review of both the Tomcat Changelog and source code determined that the changes did not affect any TSF interfaces, SFR, or security functions and resulted in minor changes to the TOE.

The installer update no longer includes the Oracle JRE. Oracle JDK/JRE must be installed and maintained independently from the TOE. Additionally, the default DN encoding was changed to increase compatibility with products that support PrintableString.

A detailed description of each change and the associated impact and rationale was provided for all the TOE changes. The rationale provided supporting evidence to ensure that the changes were either not TOE security relevant or considered minor.

Bug Fixes
Two bug fixes were identified. These fixed impacted the sending of certificates issued by an intermediate CA and database size.

A detailed description of each fix and the associated impact and rationale was provided for all bug fixes. The rationale provided supporting evidence to ensure that the fixes either were not TOE security relevant or corrected minor issues.

Changes to Evaluation Documents:

The CC Guidance contains many updates related to the supported Java/JRE and the cc-mode installation. The document also indicates the following documents have been updated for this assurance maintenance.

Regression Testing:

Regression testing was performed on the TOE, using the same operational environments as the original evaluation testing and all have been reported as passing. The regression testing included new feature testing, change testing and additional other regressing testing.

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 and all tests passed.

The vendor also reported that all known vulnerabilities associated with the evaluated product releases have been addressed with this updated product release.

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