CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Information Security Corporation CertAgent/Dhuma v8.0 patch level 0.6

Maintenance Report Number: CCEVS-VR-VID11457-2025-2

Date of Activity: December 17, 2025

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." 29 August 2014.

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

Protection Profile for Certification Authorities, version 2.1 [PP_CA_V2.1]

Impact Analysis Report for CertAgent/Dhuma Version 8.0 Patch 0.6, version 1.0.1, December 17, 2025

CertAgent/Dhuma v8.0 patch level 0.6 Security Target for Common Criteria Evaluation, version 5.0.17, December 17, 2025

CertAgent/Dhuma v8.0 patch level 0.6 Guidance for Common Criteria Evaluation, version 3.0.10, December 17, 2025

Affected Developer Evidence and Documentation Updates:

The following table shows how the documentation has been updated from the previous Assurance Maintenance activity for CertAgent/Dhuma v8.0 patch level 0.4 to CertAgent/Dhuma v8.0 patch level 0.6:

Table 1: Updated Documentation

Evidence Identification	Effect on Evidence / Description of Changes

Security Target: CertAgent/Dhuma v8.0 patch level 0.4 Security Target for Common Criteria Evaluation, version 5.0.14, January 4, 2025	**Updated Security Target:** CertAgent/Dhuma v8.0 patch level 0.6 Security Target for Common Criteria Evaluation, version 5.0.17, December 17, 2025 • Updated TOE references from version from patch level 0.4 to 0.6 • Updated TOE Documentation versions/dates • Updated reference to Java JRE from version 17.1.12 to 17.1.17 • Added reference to additional Firefox ESR browser version
Guidance for Common Criteria Evaluation: CertAgent/Dhuma v8.0 patch level 0.4 Guidance for Common Criteria Evaluation, version 3.0.7, January 3, 2025	**Updated Guidance for Common Criteria Evaluation:** CertAgent/Dhuma v8.0 patch level 0.6 Guidance for Common Criteria Evaluation, version 3.0.10, December 17, 2025 • Updated TOE references from version from patch level 0.4 to 0.6 • Updated TOE Documentation versions/dates • Updated reference to Java JRE from version 17.1.12 to 17.1.17 • Updated reference to Apache Tomcat from version 9.0.91 to 9.0.104 • Updated version of Firefox ESR • Editorial changes
Installation, Configuration, and Management Guide: CertAgent/Dhuma Installation, Configuration and Management Guide, version 8.0, January 3, 2025	**Updated Installation, Configuration, and Management Guide:** CertAgent/Dhuma Installation, Configuration and Management Guide, version 8.0, October 8, 2025 • Updated TOE references from version from patch level 0.4 to 0.6 • Updated reference to Apache Tomcat from version 9.0.91 to 9.0.104
Administrator Guide: CertAgent/Dhuma Administrator Guide, version 8.0, January 3, 2025	**Updated Administrator Guide:** CertAgent/Dhuma Administrator Guide, version 8.0, October 8, 2025 • Updated TOE references from version from patch level 0.4 to 0.6 • Updated reference to Apache Tomcat from version 9.0.91 to 9.0.104
Certificate Authority Guide: CertAgent Certificate Authority Guide, version 8.0, January 3, 2025	**Updated Certificate Authority Guide:** CertAgent Certificate Authority Guide, version 8.0, October 8, 2025 • Updated TOE references from version from patch level 0.4 to 0.6 • Updated reference to Apache Tomcat from version 9.0.91 to 9.0.104

Public Site Guide: CertAgent Public Site Guide, version 8.0, January 3, 2025	**Updated Certificate Authority Guide:** CertAgent Public Site Guide, version 8.0, October 8, 2025 • Updated TOE references from version from patch level 0.4 to 0.6 • Updated reference to Apache Tomcat from version 9.0.91 to 9.0.104
Release Notes: CertAgent/Dhuma Release Notes, version 8.0.0.4, January 3, 2025	**Updated Release Notes:** CertAgent/Dhuma Release Notes, version 8.0.0.6, October 8, 2025 • Updated TOE references from version from patch level 0.4 to 0.6 • Updated reference to Apache Tomcat from version 9.0.91 to 9.0.104

Updated Developer Environment:

There have been no changes to the development environment.

Description of Changes:

Information Security Corporation (ISC) submitted an IAR for approval to update the CertAgent/Dhuma v8.0 patch level 0.6 TOE from the previous Assurance Maintenance dated March 10, 2025.

This assurance maintenance covers the cumulative updates in CertAgent/Dhuma v8.0 patch level 0.5 and patch level 0.6. Changes are limited to the remediation of published vulnerabilities, minor functional enhancements, and bug fixes, none of which impact the TOE's security functionality.

Updates include vulnerability-related updates to third-party components, minor CertAgent/Dhuma functionality improvements, and guidance documentation revisions to improve clarity and reflect current third-party component versions. No changes were made to TSF interfaces, the TSF platform, SFRs, assumptions, or security objectives, and no new security functionality was introduced.

The sections below describe the individual changes to the TOE. ISC has evaluated each change and determined that they are minor both individually and in aggregate. The guidance documentation and Security Target have been updated accordingly to accurately reflect the current TOE implementation.

Changes to TOE:

The following changes to the TOE were made because they addressed published vulnerabilities, improved maintainability, or were requested by our customers. Each change was evaluated individually and in aggregate to determine its impact on the TOE's security functionality and assurance evidence.

- Updated Apache Tomcat

The third-party TOE component Apache Tomcat has been updated from version 9.0.91 to version 9.0.104 to address published vulnerabilities and implementation defects.

Table 2: Apache Tomcat Changes

Version	Change	Analysis
9.0.94	Improve performance of ApplicationHttpRequest.parseParameters()	Minor internal code optimization related to parsing data submitted to the server.
9.0.98	Refactor duplicate code for extracting media type and subtype from content-type into a single method	Minor internal refactoring of request content-type parsing logic.
9.0.99	• Optimized parameter map creation for included requests • Refactored RequestDispatcher creation • Fixed rare NullPointerException in Http11InputBuffer	Minor internal refactoring and defect correction related to HTTP request data handling.

The Apache Tomcat changes applicable to the TOE consist exclusively of internal code refactoring, performance optimizations, and defect corrections related to request and data handling. These changes do not introduce or modify any TSF interfaces, do not affect any Security Functional Requirements (SFRs), and do not alter the TOE's security functionality. No additional assurance activities are associated with these changes.

Based on ISC's review of the Apache Tomcat changelog and corresponding source code, the update is assessed as having a minor impact on assurance, as the changes are limited in scope and do not affect the security-relevant behavior or interfaces of the TOE.

- Support Oracle or Temurin Java 17, 21 and 25 only

In previously evaluated/maintained TOE versions, the TOE allowed the operational environment JDK component to be Oracle JDK/JRE, OpenJDK, Amazon Corretto, AdoptOpenJDK, and other JDK distributions provided the version was 17.0.8 or later, as these were considered functionally equivalent.

In the updated TOE version, the TOE continues to allow the use of any Java 17.0.8+–compatible JDK in the operational environment. However, Oracle and Eclipse Temurin Java versions 17.0.8+, 21, and 25 (Long-Term Support releases) are the only JDK distributions that have been explicitly tested and verified by ISC for use with the TOE. During installation, if a Java distribution or version other than Oracle or Temurin Java 17, 21, or 25 is detected, the installer issues a warning indicating that the selected Java version is untested and recommends using a tested Oracle or Temurin JDK. The warning does not prevent installation or operation of the TOE.

When this warning is displayed during installation, the local administrator is prompted to select one of the following options:

  - Abort the installation

- Continue the installation using an existing supported Java version
- Continue the installation using an untested Java version

If the TOE is installed using an untested Java version, the same warning will be displayed when performing the following actions:

- Setting the system PIN
- Running the ‘certagent.sh/.bat version’ command
- Accessing the "About" page on the Administrative site

These warnings serve as reminders to administrators to migrate to a tested Java configuration as soon as practicable.

This change was introduced in response to interoperability issues identified during testing and through customer feedback. With more than 1,000 TOE deployments using a wide range of Java distributions, this change encourages administrators to adopt a tested Java configuration, helping to reduce potential compatibility issues and minimize technical support cases related to Java version inconsistencies.

This change does not affect any TSF interfaces, SFRs, or security functions, and there are no associated assurance activities. ISC rates the impact on assurance as minor, as Java is not part of the TOE and the change only tightens the guidance and validation applied to the operational environment Java version.

- Added option to update the serial number from the Administrative site

In previously evaluated/maintained TOE versions, upgrading from an evaluation copy to a licensed copy required a local administrator to manually update a TOE configuration file with a valid serial number and restart the TOE service. This process resulted in a service interruption and limited administrative flexibility.

In the updated TOE version, a new option has been added to the existing "About" page of the Administrative site that allows administrators authorized to access the Administrative site to update the serial number remotely without requiring a TOE service restart. This enhancement was implemented in response to customer feedback and enables a more streamlined transition to a licensed copy while maintaining service availability.

This change does not modify any TSF interfaces, does not affect any Security Functional Requirements (SFRs), and does not alter the TOE’s security functionality. No additional assurance activities are required. ISC assesses the impact on assurance as minor, as this update merely provides an alternative administrative mechanism for performing an existing management function that was previously available only through manual local configuration.

- Bug Fixes

The following changes were made to correct defects in the TOE. Each defect correction restores intended behavior without introducing new functionality or altering existing security-relevant processing.

- Download links in the CA Resources page now work properly if the public site is not configured to use the default 443 port

In previously evaluated/maintained TOE versions, the download links presented on the CA Resources page were statically configured to use the default HTTPS port (443), regardless of the public site port selected during installation. When the TOE was configured to use a non-default public site port, this behavior could result in inaccessible download links.

In the updated TOE version, this defect has been corrected. The download links on the CA Resources page now correctly reflect the configured public site port, ensuring proper functionality whether the default port or a custom port is used.

This fix does not modify any TSF interfaces, does not affect any Security Functional Requirements (SFRs), and does not alter the TOE's security functionality. No additional assurance activities are required. ISC assesses the impact on assurance as minor, as the change solely corrects URL construction and port handling for existing resources and does not affect HTTPS usage, authentication mechanisms, or any security-relevant behavior of the TOE.

- Custom installation now validates the serial number properly

The TOE supports both default and custom installation modes. In the default installation mode, which is used for NIAP-compliant deployments, configuration parameters are provided interactively during installation. In the custom installation mode, configuration parameters – including the serial number – may be specified in advance within a configuration file and applied automatically during installation.

In previously evaluated/maintained TOE versions, validation of the serial number provided in the custom installation configuration file could result in the installation process aborting due to an unsatisfied link error.

In the updated TOE version, this defect has been corrected. Serial numbers provided during custom installation are now validated correctly, and the installation completes successfully when a valid serial number is supplied.

This fix does not modify any TSF interfaces, does not affect any Security Functional Requirements (SFRs), and does not alter the TOE's security functionality. No additional assurance activities are required. ISC assesses the impact on assurance as minor, as the change solely corrects a defect in serial number validation during custom installation. The resulting TOE configuration is equivalent to that of the validated and maintained TOEs, and the default installation mode already handled serial number validation correctly.

- New OCSP signer certificate can now be installed properly

In previously evaluated/maintained TOE versions, attempting to install a new delegated OCSP signer certificate for a CA account could cause the operation to hang due to a JavaScript error. As a workaround, the issuer's credential could be configured to act as the OCSP signer for generating OCSP responses.

In the updated TOE version, this defect has been corrected. A new delegated OCSP signer certificate can now be installed successfully and used to sign OCSP responses.

This fix does not affect any TSF interfaces, does not affect any Security Functional Requirements (SFRs), and does not alter the TOE's security functionality. No additional assurance activities are required. ISC assesses the impact on assurance as minor, as the change corrects a user interface defect and restores the intended capability without changing how the TOE processes OCSP requests or generates OCSP responses.

- Use of existing ECC credentials as the system credential

In previously evaluated/maintained TOE versions, attempting to switch the system credentials to existing Elliptic Curve Cryptography (ECC) credentials already resident on the PKCS#11 Cryptographic Module could result in an error indicating that the key type was unsupported. As a result, administrators were required to generate and assign a new set of ECC credentials to configure the TOE to use ECC-based system credentials. This behavior was caused by a string comparison failure resulting from a change in the key type string returned by the certificate processing engine.

In the updated TOE version, this defect has been corrected by updating the list of allowed key type strings used when validating that the selection is a valid key type. Existing ECC system credentials can now be applied successfully without requiring them to be newly generated.

This fix does not modify any TSF interfaces, does not affect any Security Functional Requirements (SFRs), and does not alter the TOE's security functionality. No additional assurance activities are required. ISC assesses the impact on assurance as minor, as the change corrects a defect and restores the intended administrative capability of selecting existing ECC credentials as the system credential. The fix does not alter the cryptographic key establishment or signing operations, does not introduce new algorithms, and does not change the cryptographic modules used; therefore, no additional cryptographic algorithm testing is required.

- Inclusion of Subject Alternative Names from the Upload Page and Certificate Request

In previously evaluated/maintained TOE versions, when a CA account was configured to accept Subject Alternative Names (SANs) from both the Upload page and submitted certificate requests, only the SANs provided in the certificate request were included in the issued certificate. SANs specified via the Upload page were not included.

In the updated TOE version, this defect has been corrected. When permitted by the CA account configuration, all SANs specified through both the Upload page and the certificate request are now properly included.

This fix does not modify any TSF interfaces, does not affect any Security Functional Requirements (SFRs), and does not alter the TOE's security functionality. No additional assurance activities are required. ISC assesses the impact on assurance as minor, as the change corrects a defect in certificate content processing and does not alter certificate validation, issuance policy enforcement, or any other security-relevant behavior of the TOE.

- Resolution of Connection Pool Timeout Caused by Invalid Public Site Search Requests

In previously evaluated/maintained TOE versions, when a crafted request containing invalid input (i.e., one not generated through the user interface) was submitted to the Public Site's Search page, an appropriate error message was returned. However, in the event of such an error, the database connection obtained from the connection pool was not released. Repeated submission of invalid crafted requests could eventually exhaust the available database connections, resulting in a connection pool timeout and causing the TOE to shut down.

In the updated TOE version, this defect has been corrected. Database connections are now properly released when an error occurs, and input validation has been moved to an earlier stage in request processing, prior to obtaining a database connection. This prevents unnecessary resource usage and eliminates the possibility of connection pool exhaustion due to invalid search requests.

This fix does not modify any TSF interfaces, does not affect any Security Functional Requirements (SFRs), and does not alter the TOE's security functionality. No additional assurance activities are required. ISC assesses the impact on assurance as minor, as the change corrects an internal resource management defect and improves robustness without altering certificate search functionality, access controls, or any security-relevant behavior of the TOE.

Equivalency

The TOE changes fixed defects, simplified the configuration process, clarified and tightened validation of Java operational environment requirements, and improved internal data handling. There are no changes to the TSF interfaces, SFRs, or security functions. There are no assurance activities associated with the changes.

Assurance Continuity Maintenance Report:

- Information Security Corporation submitted an Impact Analysis Report (V1.0.1) to update the TOE from version 8.0 patch level 0.4 to version 8.0 patch level 0.6.
- Updates consist of updating Apache Tomcat, updates to support Oracle or Temurin Java 17, 21 and 25 only, added option to update the serial number from the Administrative site, and bug fixes.

- The updated TOE cryptographic modules have not changed and remain applicable, therefore no updates to the CAVP certificate(s) were required.
- There are no security relevant updates, so no new certification is required.
- No development environment changes occurred that impacted the product.
- There were no changes that required the evaluators to do any additional assurance activity testing.

Description of Regression Testing:

Information Security Corporation performed regression testing on the changed TOE in the same operational environments (Windows Server 2019 and RHEL 9.2) as the validated and maintained TOEs. Regression testing covered all updates and bug fixes made to the updated TOE. In all cases, the TOE behavior was consistent with the validated and maintained TOEs. There were no assurance activities associated with these changes, however, some SFR tests were performed as part of regression testing.

Vulnerability Assessment:

The public vulnerability search covers the period between the previous Assurance Maintenance activity search on 3/7/2025 and the updated search performed on 12/17/2025. The evaluator searched the following public vulnerability databases:

maintained, and changed TOE using the following resources:

- NIST NVD (National Vulnerability Database) https://nvd.nist.gov/vuln/search
- MITRE CVE https://www.cve.org
- CISA KEV https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Apache Tomcat 9.x vulnerabilities: https://tomcat.apache.org/security-9.html

with the following search terms:

- "CertAgent"
- "Information Security Corporation CertAgent "
- "ISC's Cryptographic Development Kit "
- "ISC CDK DRBG "
- "ISC CDK "
- "Apache Tomcat 9.0.84"
- "Apache Tomcat"
- "Dhuma "
- "information security corporation"
- "JDK 17.0.12"
- "JDK 17.0.17"
- "Oracle Java 17.0.12"
- "Oracle Java 17.0.17"
- "Thales TCT T-5000 Luna Network HSM model VBD-T7 firmware version 7.11.1"
- "HyperSQL "
- "PostgreSQL 15.7"

- "PostgreSQL postgresql_jdbc_driver "
- "RedHat Enterprise 9.2"
- "Windows Server 2019"
- “Apache Log4j2”
- “com.google.code.gson”
- “jQuery 3”
- “jQuery UI”

The IAR contains the output from the vulnerability searches and the rationale why the search results are not applicable to the TOE. No vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE via TOE update covered by this assurance maintenance.

Vendor Conclusion:

The vendor concludes that the assurance impact is **minor**. There are no changes to the TSF interfaces, SFRs, or security functions. There are no assurance activities associated with the changes. The testing performed by ISC covers the changes, all SFRs that were related to the changes, and most of the other SFRs and shows that the updated version still meets the PP.

Validation Team Conclusion:

The validation team reviewed the changes and concurred the changes are **minor**, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The Security Target, Common Criteria Guidance Document, and other guidance documents were changed in accordance with the descriptions in Table 1, and no additional CAVP certificates were required.

Based on this and other information from within the IAR document, the Validation Team agrees that the assurance impact of these changes is **minor**.