ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Information Security Corporation CertAgent/Dhuma v8.0 patch level 0.4

Information Security Corporation CertAgent/Dhuma v8.0 patch level 0.4

Maintenance Report Number: CCEVS-VR-VID11457-2025

Date of Activity: 10 March 2025

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, September 2008.

Information Security Corporation CertAgent/Dhuma Impact Analysis Report for Common Criteria Assurance Maintenance Update from Version 8.0, Patch Level 0.3 to Version 8.0, Patch Level 0.4, Version 1.0.0, 7 March 2025.

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

Documentation updated:

The following table shows how the original documentation has been updated:

Evidence Identification	Effect on Evidence / Description of Changes
Security Target: CertAgent/Dhuma v8.0 patch level 0.3 Security Target for Common Criteria Evaluation, version 5.0.13, 9 September 2024	**Maintained Security Target:** CertAgent/Dhuma v8.0 patch level 0.4 Security Target for Common Criteria Evaluation, version 5.0.14, 4 January 2025.
Guidance for Common Criteria Evaluation: CertAgent/Dhuma v8.0 patch level 0.3 Guidance for Common Criteria Evaluation, version 3.0.5,9 September 2024	**Maintained Guidance for Common Criteria Evaluation:** CertAgent/Dhuma v8.0 patch level 0.4 Guidance for Common Criteria Evaluation, version 3.0.7, 3 January 2025

Installation, Configuration and Management Guide: CertAgent/Dhuma Installation, Configuration and Management Guide, Version 8.0, July 30, 2024.	**Maintained Installation, Configuration and Management Guide:** CertAgent/Dhuma Installation, Configuration and Management Guide, Version 8.0, July 30, 2024.
Administrator Guide: CertAgent/Dhuma Administrator Guide, Version 8.0., 30 July 2024.	**Maintained Administrator Guide:** CertAgent/Dhuma Administrator Guide, version 8.0, 3 January 2025
Certificate Authority Guide: CertAgent Certificate Authority Guide, version 8.0, July 22, 2024	**Maintained Certificate Authority Guide:** CertAgent Certificate Authority Guide, version 8.0, 3 January 2025
Public Site Guide: CertAgent Public Site Guide, version 8.0, 22 July 2024	**Maintained Public Site Guide:** CertAgent Public Site Guide, version 8.0, 3 January 2025
Release Notes: CertAgent/Dhuma Release Notes, version 8.0.0.3, 28 July 2024	**Maintained Release Notes:** CertAgent/Dhuma Release Notes, version 8.0.0.4, 3 January 2025

1 Summary Description of Changes

There were no changes made to the TSF interfaces, TSF platform, SFRs, assumptions, or security objectives and no new security functions were added. The sections below describe the changes to the TOE. ISC has evaluated each and, in our opinion, they are all minor individually and in total. The guidance and security target documents have been updated to reflect the changes to the TOE.

The TOE modifications are divided into Changes and Bug Fixes. The primary driver of all the modifications was ease of use and maintenance, based on customer feedback.

1.1 TOE Changes

The following changes to the TOE were made because they improved maintainability, addressed common usability issues, or were requested by our customers.

- Added an option to remove a certificate request generated in the CA Credential, OCSP Credential, or Dhuma Account pages.

In the previous versions, certificate requests generated in the CA Credential, OCSP credential and Dhuma Account pages could not be removed. Customers reported accidentally generating a CA certificate request on a CA account which already had a valid credential. They wanted guidance on how to remove the request because each time an administrator would log into the CA account a warning message would appear saying a certificate request was generated and asking them to check the status of the request. The certificate request information and warning message remain until the associated issuer certificate is imported to replace the certificate request.

In this version, an option has been added to the CA Credential page to allow the removal of a newly generated certificate request which does not have a certificate associated with it. In addition, the same option has been added to the OCSP Credential and Dhuma Account pages to remove newly generated certificate requests that do not have a certificate associated with them.

This change is based on customer feedback. This option allows customers to remove any certificate requests that were incorrectly created, created by mistake, or are no longer needed.

This change does not affect the TSF interface, SFRs, or security functions. ISC rates the impact on assurance as minor because it only allows the removal of a certificate request and does not affect the current signing credential associated with the account.

- If the NIAP conformance option ‘Accepting Certificate Requests using SHA-256, SHA-384, and SHA-512 only’ is disabled, it now accepts SHA-1 signed requests in addition to SHA-224.

  Version 8.0 patch levels 0.2 and 0.3 do not accept certificate requests whose signature uses SHA-1 even if the NIAP conformance option page’s setting ‘Accepting Certificate Requests using SHA-256, SHA-384, and SHA-512 only’ is disabled. In those versions, disabling this option still only allows certificate requests whose signature uses SHA-224 in addition to SHA-256, SHA-384, and SHA-512.

  In this version, if the NIAP conformance option ‘Accepting Certificate Requests using SHA-256, SHA-384, and SHA-512 only’ is disabled, it will accept certificate requests whose signatures use SHA-1 , SHA-224, SHA-256, SHA-384, or SHA-512. Like the other options on the NIAP conformance page, this option must be enabled for the TOE to operate in NIAP mode and be compliant. If this option is disabled, the TOE will not be operating in NIAP mode, but certificate requests whose signatures use SHA-1, SHA-224, SHA-384, or SHA-512 will be accepted. If the option is enabled, the TOE continues to only accepts certificate requests whose signatures use SHA-256, SHA-384, or SHA-512.

  This change is based on customer feedback. This option allows customers to operate the TOE in non-NIAP mode in order to serve existing client applications until they can be updated to generate certificate requests whose signatures use SHA-256, SHA-384, or SHA-512 and are compliant with the TOE running in NIAP mode.

These changes do not affect the TSF interface, SFRs, and security functions. ISC rates the impact on assurance as minor because the TOE behaves identically to the validated and maintained TOEs when this option is checked, as it must be in order for the TOE to run in NIAP compliant mode.

1.2 Bug Fixes

The following changes were made to correct defects in the TOE.

- Correct a race condition on RHEL which occasionally resulted in incorrect date values when formatting dates during certificate issuance, CRL issuance, and OCSP response generation.

  A customer generating a high volume of certificates reported that occasionally certificates issued via RAMI had a notBefore and/or notAfter date different from the expected value. Investigation revealed a race condition on RHEL systems in the function that creates ASN.1 encoded dates when processing a lot of requests (issuing certificates or CRLs via RAMI or signing OCSP responses). When multiple threads attempted to ASN.1 encode a date they would occasionally interfere with each other and the date values placed in issued certificates, CRLs, and OCSP responses would be different than requested or expected.

  The code was updated to be thread safe. The date fields in the signed certificates, CRLs and OCSP responses are now set properly.

  This change does not affect any TSF interfaces, SFRs, or security functions. ISC rates the impact on assurance as minor because all dates are now formatted properly, and the race condition has been corrected.

- Improve page validation and filters user data to prevent XSS attacks.

  In the previous versions, some of the web pages didn’t filter user input data and might suffer from XSS (cross-site scripting) attacks. In this version, page validation has been improved on both client and server sides to reject invalid inputs. User input data is now properly sanitized before it is displayed on the web pages.

  These changes do not affect the TSF interface, SFRs, or security functions and there are no assurance activities associated with this change. ISC rates the impact on assurance as minor because this bug fix does not change security functionality or affect any SFRs.

- Update the background color of the evaluation banner to comply with the WCAG AAA requirements.

  If CertAgent/Dhuma serial number is not entered during the installation, the TOE will run in evaluation mode. An evaluation banner will appear on the top of each web pages.

  In the previous versions, the background color of the evaluation banner did not comply with the WCAG AAA requirements. In this version, the background color of the banner has been tuned to comply with the requirements.

  These changes do not affect the TSF interface, SFRs, or security functions and there are no assurance activities associated with this change. ISC rates the impact on assurance as minor because this bug fix does not change security functionality or affect any SFRs. Valid CertAgent and Dhuma serial numbers are entered in NIAP compliant TOE which is the same as the validated and maintained TOEs.

- Submitting a certificate request with no subject DN via RAMI no longer returns a database error and shuts down the TOE

  In the previous versions, if the TOE was installed with the “NIAP Compliance” option unchecked and configured to use an Oracle database, submitting a certificate request with no subject DN via the Registration Authority Management Interface (RAMI) would return a database error and shut down the TOE. If the TOE was installed with an evaluated configuration using HyperSQL or PostgreSQL, submitting such a request via RAMI by an authorized RA would properly enroll successfully.

  This version corrects the defect in the non-NIAP compliant installation when using an Oracle database by changing how empty DNs are stored in the database. The evaluated and maintained TOEs stored an empty DN as the empty string which Oracle does not support. The changed TOE now uses “(not set)” instead for all supported databases. When reading entries back from the database the empty string and “(not set)” are treated in the same manner by the changed TOE.

  With the changed TOE running in non-NIAP mode, submitting a certificate request without a DN via RAMI now enrolls successfully with Oracle just as it does in the validated and maintained TOEs running in NIAP-mode with HyperSQL or PostgreSQL.

  This change does not affect the TSF interface, SFRs, or security functions. ISC rates the impact on assurance as minor because this change corrects the defect with an internal change to how data is stored in the database. This change does not affect any of the security claims within the evaluation and the RAMI interface is unchanged.

1.3 Developer Environment and Evidence

No changes were made to the development environment.

The following developer evidence was impacted:

- The AGD document named "CertAgent/Dhuma Guidance for Common Criteria Evaluation" has been updated to version 3.0.7, January 3, 2025.

- The Security Target document named "CertAgent/Dhuma Security Target for Common Criteria Evaluation" has been updated to version 5.0.14, January 4, 2025.

The changes made to the TOE meet all applicable NIAP policies. The Guidance and Security Target documents have been updated to reflect the changes made.

The installation includes the updated TOE version number (8.0.0.4). Therefore, Guidance document sections 1.2.1, 3.2, 3.2.1, 4.9, 4.10.1, 4.10.2, 4.10.4, 4.10.5, and 4.12.1.3 have been updated to reflect the changes.

The AGD document named "CertAgent/Dhuma Guidance for Common Criteria Evaluation" has been updated to version 3.0.7, January 3, 2025.

CertAgent/Dhuma Security Target for Common Criteria Evaluation has been updated to version 5.0.14, January 4, 2025.

2 Regression Testing

Regression tests have been performed on the changed TOE in the same operational environments (Windows Server 2019 and RHEL 9.2) and Java version (17.0.12) as the validated and maintained TOEs. All tests passed.

2.1 Tests of the Changes

- An option was added to remove the certificate request generated in the CA Credential, OCSP Credential, and Dhuma Account pages. We confirmed that if a certificate request has been generated in the CA Credential, OCSP Credential, and Dhuma Account pages:

  A remove certificate request option appeared in the page.

  if the remove certificate request option was selected, it only removed the certificate request from the associated page. The active credential (if existed) remained functional. A warning message no longer appeared when login to the account.

There are no assurance activities associated with these changes.

- If the NIAP conformance option ‘Accepting Certificate Requests using SHA-256, SHA-384, and SHA-512 only’ is disabled, it now accepts SHA-1 signed requests in addition to SHA-224.

  We generated different combinations of RSA-3072 and ECDSA P-384 certificate requests signed using SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 and repeatedly submitted them to the TOE via EST, the Public site and RAMI. We verified that the TOE accepted all certificate requests when the ‘Accepting Certificate Requests using SHA-256, SHA-384, and SHA-512 only’ option was disabled, and rejected all SHA-1, and SHA-224 signed certificate requests if this option was enabled.

  In the regression test, the changed TOE rejected all SHA-1, and SHA-224 signed certificate requests which is the same as was done for the validated and maintained TOEs. This change was tested by performing the tests in FCO_NRO_EXT.2 Certificate-Based Proof of Origin, FDP_CER_EXT.3.1 Certificate Issuance Approval, FIA_ESTS_EXT.1 Enrollment over Secure Transport (EST) Server and verifying the results.

  There are no assurance activities associated with this change.

2.2 Defect Correction Testing

- Corrects a race condition on RHEL which occasionally resulted in incorrect date values when formatting dates during certificate issuance, CRL issuance, and OCSP response generation.

  The issue was most easily replicated by repeatedly submitting several hundred certificate requests using multiple threads on a RHEL system. We verified the new version behaved correctly on both RHEL and Windows systems by

  - Submitting more than one million (1,000,000) certificate enrollment requests via RAMI using multiple threads simultaneously and verifying that the issued certificates have the correct notBefore and notAfter dates based on the issuance time and configured validity period,

  - Submitting more than one million (1,000,000) EST simpleenroll requests using multiple threads simultaneously and verifying that the issued certificates have the correct notBefore and notAfter dates based on the issuance time and configured validity period,

  - Submitting more than one million (1,000,000) OCSP requests using multiple threads simultaneously and verifying that OCSP responses have the correct producedAt, thisUpdate, and nextUpdate dates based on the OCSP signing time and the configured next update time, and the OCSP client was able to use the responses, and

  - Submitting more than one million (1,000,000) CRL issuance requests via RAMI using multiple threads simultaneously and verifying that the issued CRLs have the correct thisUpdate and nextUpdate dates based on the issuance time and configured validity period.

  In the regression test, this change was tested by performing the tests in FDP_OCSPG_EXT.1 OCSP Basic Response Generation, FIA_ESTS_EXT.1 Enrollment over Secure Transport (EST) Server, FDP_CER_EXT.1 Certificate Profiles, FDP_CER_EXT.3.1 Certificate Issuance Approval, and FDP_CRL_EXT.1 Certificate Revocation List Validation and verifying the results.

- Improves page validation and filters user data to prevent XSS attacks
  All the affected web pages were tested with a malicious script as input and the results verified. There are no assurance activities associated with these changes.

- Updates the background color of the evaluation banner to comply with the WCAG AAA requirements.

  We verified that the background color of the evaluation banner complied with the WCAG AAA requirements using the WAVE extension (Web Accessibility Evaluation Tools) in Firefox. There are no assurance activities associated with these changes.

- Submitting a certificate request with no subject DN via RAMI no longer returns a database error and shuts down the TOE.

  The TOE was repeatedly installed in different configurations:
  - NIAP compliance option with a HyperSQL database
  - NIAP compliance option with a PostgreSQL database
  - Non-NIAP compliance option with a HyperSQL database
  - Non-NIAP compliance option with a PostgreSQL database
  - Non-NIAP compliance option with an Oracle database

  For each configuration we verified that certificate requests with no subject DN could enroll successfully via RAMI and that certificate requests with a subject DN could enroll successfully through all interfaces.

  This change was tested by performing the FDP_CER_EXT.3 Certificate Issuance Approval tests and verifying the results.

2.3 Other Regression Testing

In addition to the tests conducted to ensure the changes made were correct and did not introduce new defects, ISC performed tests covering SFRs: FAU_ADP_EXT.1, FAU_GCR_EXT.1, FAU_SCR_EXT.1, FAU_SAR.1, FAU_SEL.1, FDP_CSI_EXT.1, FDP_CRL_EXT.1, FIA_X509_EXT.3, FMT_MOF.1(1), FMT_MTD.1, FMT_SMF.1, FPT_TUD_EXT.1, and FTA_TAB.1.

3 Assurance Activity Coverage Argument

The TOE changes which had associated assurance activities only fixed defects. There are no changes to the TSF interfaces, SFRs, or security functions.

4 Vulnerability Coverage Argument

On March 7, 2025, ISC performed a vulnerability assessment on the libraries that have not been changed since the maintained TOE, using the NIST National Vulnerability Database (https://nvd.nist.gov/vuln/search).

4.1 Apache Tomcat

Apache Tomcat 9.0.91 has not been changed in the TOE. “Apache Tomcat 9” search term was used in the NIST National Vulnerability Database (https://nvd.nist.gov/vuln/search) and found 83 potential vulnerabilities. Among the 83 vulnerabilities, only 4 of them applied to Apache Tomcat 9.0.91 (used in the changed and maintained TOEs). The table below lists each potential vulnerability identified, its applicability to the TOE, and the Tomcat version that addressed the vulnerability:

CVE	Analysis	Fixed in Version
CVE-2024-56337	Not applicable: The TOE uses the default servlet configuration	9.0.99
CVE-2024-54677	Not applicable: The TOE doesn’t include the examples web application	9.0.98
CVE-2024-50379	Not applicable: The TOE uses the default servlet configuration	9.0.98
CVE-2024-52316	Not applicable: The TOE doesn’t use any custom Jakarta Authentication	9.0.96

The above vulnerabilities have been addressed in version 9.0.96, 9.0.98, or 9.0.99 (not the version used by the changed TOE), but they don’t apply to the changed or maintained TOEs.

4.2 Other Libraries

The table below lists each potential vulnerability identified and its applicability to the TOE. None of the CVEs were found applicable to the TOE. The following search terms were used which cover the components libraries used by the TOE:

- Apache Log4j2 (4)
- CDK (4)
- com.google.code.gson (1)
- jQuery 3 (13)
- jQuery UI (10)

CVE	Search Term	Analysis
CVE-2023-50780	Apache Log4j2	Not applicable: The TOE doesn’t use Apache ActiveMQ Artemis
CVE-2021-45105		Not applicable: doesn’t apply to the Apache Log4j2 2.22. library used by the TOE
CVE-2021-44832		
CVE-2021-44228		
CVE-2024-45037	CDK	Not applicable: doesn’t refer to the CDK library used by the TOE
CVE-2023-35165		
CVE-2017-7869		
CVE-2017-5336		
CVE-2022-25647	com.google.code.gson	Not applicable: doesn’t apply to the gson 2.10.1 library used by the TOE
CVE-2024-32753	jQuery 3	Not applicable: doesn’t apply to the jQuery 3.7.1 library used by the TOE
CVE-2024-24850		Not applicable: the TOE does not use Mark Stockton Quicksand Post Filter jQuery Plugin
CVE-2024-24849		
CVE-2023-5432		Not applicable: the TOE does not use the JQuery news ticker plugin for WordPress
CVE-2023-5430		
CVE-2023-4890		Not applicable: the TOE does not use the JQuery Accordion Menu Widget for WordPress plugin
CVE-2020-11022		

CVE-2020-11023		Not applicable: doesn’t apply to the jQuery 3.7.1 library used by the TOE
CVE-2019-11358		
CVE-2017-6929		Not applicable: the TOE does not make Ajax requests to untrusted domain
CVE-2016-10707		Not applicable: doesn’t apply to the jQuery 3.7.1 library used by the TOE
CVE-2015-9251		Not applicable: the TOE does not make cross-domain request
CVE-2015-1840		Not applicable: the TOE does not use jquery-rails
CVE-2024-30875	jQuery UI	Not applicable: doesn’t apply to the jQuery UI 1.13.2 library used by the TOE
CVE-2022-31160		Not applicable: the TOE does not use any `.checkboxradio(“refresh”) function`
CVE-2021-41184		Not applicable: the TOE does not use any `of` option of the `.position()`
CVE-2021-41183		Not applicable: the TOE does not use any `*Text` options of the Datepicker widget
CVE-2021-41182		Not applicable: the TOE does not use the `altField` option of the Datepicker widget
CVE-2021-32682		Not applicable: the TOE does not use elFinder
CVE-2017-15719		Not applicable: the TOE doesn’t use Wicket jQuery UI
CVE-2016-7103		Not applicable: doesn’t apply to the jQuery UI 1.13.2 library used by the TOE
CVE-2012-6662		
CVE-2010-5312		

5 Conclusion

We conclude that the assurance impact is minor in the aggregate. The TOE changes which had associated assurance activities were made to fix defects. There are no changes to the TSF interfaces, SFRs, or security functions. The testing performed by ISC covers the changes, all associated SFRs, and most of the other SFRs and shows that the updated version still meets the PP.