ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
Information Security Corporation (ISC)
CertAgent/Dhuma v8.0 patch level 0.7

Maintenance Update of ISC CertAgent/Dhuma v8.0 patch level 0.6

Maintenance Report Number: CCEVS-VR-VID11457-2026

Date of Activity: 26 August 2026

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 3.0. 12 September 2016.
- ISC CertAgent Dhuma Impact Analysis Report (IAR) for Common Criteria Assurance Maintenance update from Version 8.0 patch level 0.6 to Version 8.0 patch level 0.7. 25 August 2026.
- Protection Profile for Certification Authorities, Version 2.1. 12 January 2017. [PP_CA_V2.1].

Documentation updated:

The AGD document, CertAgent/Dhuma Guidance for Common Criteria Evaluation, has been updated to version 3.0.12, August 24, 2026.

The Security Target (ST), CertAgent/Dhuma Security Target for Common Criteria Evaluation, has been updated to version 5.0.18, August 25, 2026.

The changes made to the TOE comply with applicable NIAP policies. The Guidance and Security Target documents have been updated, where applicable, to accurately reflect the changed TOE.

The following sections identify the developer evidence that has been updated.

NOTE: Only TOE changes that affect the evaluated configuration or require updates to the developer evidence are listed. Changes outside the scope of the TOE evaluation or changes that do not require updates to the developer evidence are not included.

Operational Environment Updates

The installation guidance has been updated to reflect the supported versions of the third-party non-TOE components:

- Oracle Java 17.0.20.1

- HyperSQL Database 2.7.4
- PostgreSQL Database 15.18 with JDBC Driver 42.7.11

Guidance document Sections 2, 2.5, 2.5.1, 2.5.2, 3.2, 3.2.1, 3.2.2, and 4.10.1 have been updated to reflect these changes.

Installation Updates

The installation guidance has been updated to reflect the changed TOE version (8.0.0.7) and the updated Apache Tomcat version (9.0.119).

Guidance document Sections 1.2.1, 1.2.2, 2.7, 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 these changes.

Introduction

Information Security Corporation submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 26 August 2026. 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 3.0. 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 Guidance for Maintenance and Re-evaluation, and the Impact Analysis Report (IAR). The ST and guidance document were updated, the IAR was new.

Description of the Changes

CertAgent/Dhuma remains substantially unchanged between version 8.0 patch level 0.6 and version 8.0 patch level 0.7. The changes introduced in patch level 0.7 are limited to the remediation of published vulnerabilities, third-party component maintenance updates, implementation defect corrections, and customer-requested features, none of which affect the TOE's security functionality.

The updates include third-party component updates to address published vulnerabilities and incorporate maintenance updates, implementation defect corrections, customer-requested features, and revisions to the guidance documentation to reflect the updated third-party component versions. No changes were made to the TSF interfaces, SFRs, assumptions, or security objectives, and no new security functionality was introduced.

The following sections describe the individual changes made to the TOE. ISC evaluated each change individually and collectively and determined that the overall assurance impact is minor. The guidance documentation and Security Target have been updated, where applicable, to accurately reflect the changed TOE.

TOE

The TOE modifications are categorized as either Changes or Fixed Defects. The primary drivers for these changes were the remediation of published vulnerabilities, third-party component maintenance updates, customer-requested features, and implementation defect corrections.

Changes

The following changes were made to the TOE to address published vulnerabilities, incorporate third-party maintenance updates, improve maintainability, or implement customer-requested features. Each change was evaluated individually and collectively to determine its impact on the TOE’s security functionality, TSF interfaces, SFRs, and assurance evidence.

Updated Apache Tomcat

The third-party TOE component Apache Tomcat has been updated from version 9.0.104 to version 9.0.119. ISC reviewed the changes introduced in each Tomcat release to determine their applicability and impact on the TOE using the following authoritative sources:

- Apache Tomcat 9.x Changelog

https://tomcat.apache.org/tomcat-9.0-doc/changelog.html

- Apache Tomcat Source Repository (GitHub)

https://github.com/apache/tomcat

The table below summarizes the Tomcat changes included in this update that are applicable to the TOE, along with ISC's assessment of their impact.

Version	Change	Analysis
9.0.114	"Dereference TLS objects right after closing a socket to improve memory efficiency"	Internal implementation optimization related to TLS resource management. No impact on TSF interfaces or security functionality.
9.0.117	"Fix a bug in the non-blocking flushing code for NIO+TLS that meant that a response may not be fully written until the connection is closed"	Internal defect correction affecting TLS response handling. No impact on TSF interfaces or security functionality.

The Apache Tomcat changes applicable to the TOE are limited to internal implementation optimizations and defect corrections. They do not introduce or modify any TSF interfaces, do not affect any 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, ISC considers the assurance impact to be minor, as the applicable changes are limited in scope and do not affect the security-relevant behavior, interfaces, or functionality of the TOE.

Updated Apache Log4j

The third-party TOE component Apache Log4j has been updated from version 2.22.0 to version 2.26.0. The Log4j library is used by the TOE to record startup and shutdown events, any events that occur before the database becomes accessible, and fatal error that cause the TOE to shut down in the server log.

ISC reviewed the changes introduced in each Log4j release to determine their applicability and impact on the TOE using the following authoritative sources:

- Apache Log4j Release Notes

https://logging.apache.org/log4j/2.x/release-notes.html

- Apache Log4j Source Repository (GitHub)

https://github.com/apache/logging-log4j2

ISC determined that none of the changes introduced in Apache Log4j versions 2.22.0 through 2.26.0 affect the TOE's TSF interfaces, SFRs, or security functionality.

This update was made in response to customer requests to use the latest Apache Log4j release. Although the published Apache Log4j vulnerabilities reviewed by ISC do not apply to the TOE, customers frequently report vulnerability scanner findings based solely on the presence of older Log4j versions, resulting in unnecessary technical support requests.

This update does not introduce or modify any TSF interfaces, does not affect any SFRs, and does not alter the TOE's security functionality. There are no assurance activities associated with this change. ISC considers the assurance impact to be minor because the update does not affect the security-relevant behavior or functionality of the TOE.

Updated HyperSQL Database Library

The third-party HyperSQL database library has been updated from version 2.7.2 to version 2.7.4 to incorporate enhancements, defect corrections, and maintenance updates provided by the HyperSQL project.

The HyperSQL database server is part of the operational environment and is outside the TOE boundary. The TOE includes the HyperSQL database library solely to support the optional installation and configuration of the HyperSQL database server. When selected, the installer automatically installs and configures the HyperSQL database server for use by the TOE.

This update was introduced to incorporate the latest maintenance updates and defect corrections provided by the HyperSQL project, to keep the bundled third-party component current and supported, and to improve compatibility and reliability.

This update does not introduce or modify any TSF interfaces, does not affect any SFRs, and does not alter the TOE's security functionality. There are no assurance activities associated with this change. ISC considers the assurance impact to be minor because the HyperSQL database server is outside the TOE boundary, and the updated HyperSQL database library does not affect the security-relevant behavior or functionality of the TOE.

(**Non-NIAP only**) **Do Not Shut Down the TOE on Database Error**

In previous versions, if the database became inaccessible, the TOE recorded the database error message in the local server log and then shut down to prevent further operations and potential audit data loss.

In this version, if the product is **not** installed with the "NIAP Compliance" option and the database becomes inaccessible, any TOE services that require database access are denied with an appropriate error message. The TOE records the database error message in the local server log but does not shut down. Once database connectivity is restored, those TOE services automatically resume normal operation.

If the TOE is installed with the "NIAP Compliance" option, there is no change in behavior.

This change was introduced in response to customer requests to improve service availability in non-NIAP deployments. Customers deploying the TOE in high-availability and clustered environments requested that a temporary database outage not require the TOE to shut down, thereby allowing database-independent services to remain available and normal operation to resume automatically when database connectivity is restored.

This change does not introduce or modify any TSF interfaces, does not affect any SFRs, and does not alter the TOE's security functionality. There are no assurance activities associated with this change. ISC considers the

assurance impact to be minor because the change is not enabled in the evaluated configuration, which requires the TOE to be installed with the NIAP Compliance option. When the TOE operates in the NIAP Compliance configuration, it continues to provide the same security functionality as the previously validated and maintained TOEs.

Added Support for Retrieving CRLs Using LDAP and LDAPS Protocols

In previous versions, the TOE supported retrieving CRLs from an external server using the HTTP protocol only.

In this version, if the product is **not** installed with the "NIAP Compliance" option, the TOE also supports retrieving CRLs using the LDAP and LDAPS protocols. When the LDAPS protocol is selected, the administrator must provide, in addition to the LDAPS URL, an X.509 certificate or PKCS#7 file containing one or more trust anchors. This trust anchor file is used to validate the LDAP server's certificate chain during establishment of the TLS connection.

If the TOE is installed with the "NIAP Compliance" option, there is no change in behavior.

This change was introduced in response to customer requests to support existing LDAP/LDAPS-based CRL distribution infrastructures without requiring changes to their deployment environments.

This change does not introduce or modify any TSF interfaces, does not affect any SFRs, and does not alter the TOE's security functionality. There are no assurance activities associated with this change. ISC considers the assurance impact to be minor because the change is not enabled in the evaluated configuration, which requires the TOE to be installed with the NIAP Compliance option. When the TOE operates in the NIAP Compliance configuration, it continues to provide the same security functionality as the previously validated and maintained TOEs.

Fixed Defects

The following changes were made to correct implementation defects in the TOE. Each defect correction addresses a specific implementation issue while preserving the TOE's existing security functionality. These changes do not introduce or modify any TSF interfaces, do not affect any SFRs, and do not alter the TOE's security functionality.

Correct PKCS#11 C_Finalize() Invocation

A new HSM vendor reported that the TOE installer crashed during interoperability testing. Investigation determined that the TOE invoked the PKCS#11 C_Finalize() function multiple times during installation and server startup. This behavior is not compliant with the PKCS#11 specification and was not tolerated by the vendor's PKCS#11 library.

The TOE was updated to invoke C_Finalize() only when installation is complete or when the TOE shuts down, consistent with the PKCS#11 specification. Following this change, the TOE no longer crashes when used with the new HSM. The Thales TCT HSM used in the validated and maintained TOEs continues to operate correctly with the changed TOE.

This change does not introduce or modify any TSF interfaces, does not affect any SFRs, and does not alter the TOE's security functionality. There are no assurance activities associated with this change. ISC considers the assurance impact to be minor because the change corrects a standards-compliance defect without altering the TOE's PKCS#11 functionality or security behavior.

Addressed Database Deadlock in PostgreSQL During CRL Issuance

A customer reported a database deadlock when issuing CRLs. Investigation determined that, in PostgreSQL, a deadlock could occur when multiple transactions attempted to update the status of the same set of certificates simultaneously while processing the certificate IDs in different orders. This behavior was not observed with HyperSQL or Oracle databases.

To eliminate the possibility of deadlocks, the TOE was updated to sort the certificate IDs before updating their status. Processing the certificate IDs in a consistent order prevents conflicting lock acquisition sequences and eliminates the PostgreSQL deadlock condition.

This change does not introduce or modify any TSF interfaces, does not affect any SFRs, and does not alter the TOE's security functionality. There are no assurance activities associated with this change. ISC considers the assurance impact to be minor because the change corrects a database concurrency issue without altering the TOE's certificate revocation processing, CRL issuance, or security functionality.

Affected Developer Evidence

The AGD document, CertAgent/Dhuma Guidance for Common Criteria Evaluation, has been updated to version 3.0.12, August 24, 2026.

The Security Target (ST), CertAgent/Dhuma Security Target for Common Criteria Evaluation, has been updated to version 5.0.18, August 25, 2026.

The changes made to the TOE comply with applicable NIAP policies. The Guidance and Security Target documents have been updated, where applicable, to accurately reflect the changed TOE.

The following sections identify the developer evidence that has been updated.

NOTE: Only TOE changes that affect the evaluated configuration or require updates to the developer evidence are listed. Changes outside the scope of the TOE evaluation or changes that do not require updates to the developer evidence are not included.

Operational Environment Updates

The installation guidance has been updated to reflect the supported versions of the third-party non-TOE components:

- Oracle Java 17.0.20.1
- HyperSQL Database 2.7.4
- PostgreSQL Database 15.18 with JDBC Driver 42.7.11

Guidance document Sections 2, 2.5, 2.5.1, 2.5.2, 3.2, 3.2.1, 3.2.2, and 4.10.1 have been updated to reflect these changes.

Installation Updates

The installation guidance has been updated to reflect the changed TOE version (8.0.0.7) and the updated Apache Tomcat version (9.0.119).

Guidance document Sections 1.2.1, 1.2.2, 2.7, 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 these changes.

Regression Testing:

Regression testing was performed on the changed TOE using the same evaluated operational environments as the previously validated and maintained TOEs, together with the latest supported Java and database components:

- Windows Server 2019 with HyperSQL 2.7.4 and Oracle Java 17.0.20.1
- RHEL 9.2 with PostgreSQL 15.18 (JDBC Driver 42.7.11), and Oracle Java 17.0.20.1

The testing verified that the implemented changes did not adversely affect the TOE's existing security functionality or operational behavior, and all regression tests completed successfully.

The test results demonstrated that the changed TOE continues to satisfy the applicable SFRs and that the implemented changes did not introduce any regressions in the TOE’s evaluated security functionality.

Test Details

Changes Testing

Updated Apache Tomcat

The Apache Tomcat changes applicable to the changed TOE consist solely of internal implementation improvements and defect corrections related to TLS processing and data handling. These changes do not introduce or modify any TSF interfaces, do not affect any SFRs, and do not alter the TOE's security functionality. No additional assurance activities are associated with these changes.

ISC performed regression testing of the updated Apache Tomcat component by executing tests covering the following SFRs:

- FCS_TLSS_EXT.1 TLS Server Protocol
- FCS_TLSS_EXT.2 TLS Server Protocol with Mutual Authentication
- FCS_HTTPS_EXT.1 HTTPS Protocol
- FTP_ITC.1 Inter-TSF Trusted Channel
- FTP_TRP.1 Trusted Path
- FAU_GEN.1 Audit Data Generation
- FDP_OCSPG_EXT.1 OCSP Basic Response Generation
- FIA_X509_EXT.1 Certificate Validation

- FIA_X509_EXT.2 Certificate-Based Authentication
- FIA_UAU_EXT.1 Authentication Mechanism
- FIA_UIA_EXT.1 User Identification and Authentication
- FIA_ESTS_EXT.1 Enrollment over Secure Transport (EST) Server
- FMT_SMR.2 Restrictions on Security Roles
- FTA_SSL.3 TSF-Initiated Termination
- FTA_SSL.4 User-Initiated Termination

The test results were consistent with those obtained for the previously validated and maintained TOEs, confirming that the updated Apache Tomcat component does not affect the TOE's security-relevant behavior or operational functionality.

Updated Apache Log4j

ISC verified that the updated Apache Log4j libraries correctly recorded TOE startup and shutdown events, events that occurred before the database became accessible, and fatal errors that caused the TOE to shut down in the server log.

As part of regression testing, ISC executed the tests associated with FAU_GEN.1.2 Audit Data Generation to verify this change. The test results were consistent with those obtained for the previously validated and maintained TOEs, confirming that the updated Apache Log4j libraries do not affect the TOE's audit generation or security-relevant behavior.

Updated HyperSQL Database Library

ISC verified that the updated HyperSQL database library was installed correctly and that the HyperSQL database server was successfully configured and operated as expected when the HyperSQL database option was selected during installation.

Regression testing confirmed that the TOE continued to operate as expected using the updated HyperSQL database library and that the update did not affect the TOE's security functionality or operational behavior.

This update does not introduce or modify any TSF interfaces, does not affect any SFRs, and does not alter the TOE's security functionality. There are no assurance activities associated with this change.

The test results were consistent with those obtained for the previously validated and maintained TOEs, confirming that the updated HyperSQL database library does not affect the TOE's security-relevant behavior or functionality.

(Non-NIAP only) Do Not Shut Down the TOE on Database Error

The TOE was repeatedly installed using different NIAP compliance configuration options.

When the product was **not** installed with the “NIAP Compliance” option and the database became inaccessible, ISC verified that all database-related operations were denied, appropriate error messages were returned and

recorded in the local server log, and the TOE remained operational. Once database connectivity was restored, the TOE automatically resumed normal operation.

When the TOE was installed with the "NIAP Compliance" option and the database became inaccessible, ISC verified that all database-related operations were denied, appropriate error messages were returned and recorded in the local server log, and the TOE shut down.

This change is not enabled in the evaluated configuration, which requires the TOE to be installed with the NIAP Compliance option. Therefore, there are no assurance activities associated with this change. This change does not introduce or modify any TSF interfaces, does not affect any SFRs, and does not alter the TOE's security functionality.

ISC performed regression testing covering FAU_STG.4 Prevention of Audit Data Loss. The test results were consistent with those obtained for the previously validated and maintained TOEs, confirming that the changed TOE exhibits the same behavior as the previously validated and maintained TOEs.

(Non-NIAP only) Added Support for Retrieving CRLs Using LDAP and LDAPS Protocols

The TOE was repeatedly installed using different NIAP compliance configuration options.

When the product was not installed with the "NIAP Compliance" option, ISC verified that the HTTP, LDAP, and LDAPS protocols were available when configuring CRL retrieval.

When the LDAPS protocol was selected and a valid trust anchor file was provided, ISC verified that the TOE successfully established a TLS connection to the LDAP server and retrieved the CRL. When the trust anchor file did not contain the root CA certificate required to validate the LDAP server's TLS certificate chain, the TOE returned an appropriate error message and did not retrieve the CRL.

ISC also verified that CRLs could be successfully retrieved using valid HTTP, LDAP, and LDAPS URLs.

When the TOE was installed with the "NIAP Compliance" option, ISC verified that only the HTTP protocol was available when configuring CRL retrieval. ISC also verified that CRLs could be successfully retrieved using valid HTTP URLs and that the changed TOE behaved consistently with the previously validated and maintained TOEs.

This change is not enabled in the evaluated configuration, which requires the TOE to be installed with the NIAP Compliance option. Therefore, there are no assurance activities associated with this change. This change does not introduce or modify any TSF interfaces, does not affect any SFRs, and does not alter the TOE's security functionality.

DEFECT CORRECTION TESTING

Correct PKCS#11 C_Finalize() Invocation

ISC verified that the PKCS#11 C_Finalize() function was invoked only when the installation was complete or when the TOE shut down, consistent with the PKCS#11 specification. ISC also verified that the TOE could be installed successfully, operate as expected, and shut down gracefully when used with the new HSM.

As part of regression testing, the TOE was installed using the Thales TCT HSM from the previously validated configuration. ISC verified that the installation completed successfully, the TOE operated as expected, and the

TOE shut down gracefully, confirming that the change did not affect compatibility with the evaluated HSM. The test results were consistent with those obtained for the previously validated and maintained TOEs.

This change does not introduce or modify any TSF interfaces, does not affect any SFRs, and does not alter the TOE's security functionality. There are no assurance activities associated with this change.

Addressed Database Deadlock in PostgreSQL During CRL Issuance

The database deadlock condition was reproduced using a test program that repeatedly updated the status of the same set of certificates concurrently while processing the certificate IDs in different orders. This test program simulated the certificate status update process performed during CRL issuance.

ISC verified that, when executed against the previous TOE using a PostgreSQL database, the test program consistently encountered a database deadlock within ten iterations.

ISC then executed the same test program against the changed TOE using PostgreSQL and verified that no deadlocks occurred after one million iterations. ISC also executed the test program against the HyperSQL database for one million iterations and confirmed that no deadlocks occurred.

This change does not introduce or modify any TSF interfaces, does not affect any SFRs, and does not alter the TOE's security functionality. There are no assurance activities associated with this change.

ISC also performed regression testing covering:

- FDP_CSI_EXT.1 Certificate Status Information
- FDP_CRL_EXT.1 Certificate Revocation List Validation

The test results were consistent with those obtained for the previously validated and maintained TOEs, confirming that the defect correction does not affect the TOE's certificate status management, CRL issuance, or security-relevant behavior.

Other Regression Testing

In addition to the tests conducted to verify that the implemented changes were correct and did not introduce new defects, ISC performed regression testing covering the following SFRs: FAU_ADP_EXT.1, FAU_GCR_EXT.1, FAU_SCR_EXT.1, FAU_SAR.1, FAU_SEL.1, FIA_X509_EXT.3, FDP_OCSPG_EXT.1, FMT_MOF.1(1), FMT_MTD.1, FMT_SMF.1, FPT_TUD_EXT.1, and FTA_TAB.1.

The test results were consistent with those obtained for the previously validated and maintained TOEs, confirming that the changed TOE behaves consistently with the previously validated and maintained TOEs.

Assurance Activity Coverage Argument

The TOE changes consist of third-party component updates, implementation defect corrections, and customer-requested features that are available only when the product is not installed with the NIAP Compliance option. These changes do not introduce or modify any TSF interfaces, do not affect any SFRs, and do not alter the TOE's evaluated security functionality when operating in the evaluated NIAP configuration.

The customer-requested features are not enabled in the evaluated configuration, which requires the TOE to be installed with the NIAP Compliance option. No assurance activities are associated with these features.

The regression testing covered all TSF interfaces and SFRs that could reasonably be affected by the changes, including the security functionality associated with the updated third-party components and the corrected implementation defects. The test results were consistent with those obtained for the previously validated and maintained TOEs, demonstrating that the changed TOE continues to satisfy the applicable Protection Profile (PP) requirements.

Vulnerability Analysis

On August 24, 2026, ISC performed a vulnerability assessment of the software components used by the validated, maintained, and changed TOEs using the following authoritative sources:

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

The identified potential vulnerabilities were reviewed to determine their applicability to the validated, maintained, and changed TOEs and to assess whether any additional security risks were introduced by the changes.

SEARCH TERMS

TOE Components

The table below lists the search terms used to identify vulnerabilities for the TOE components included in the evaluated TOE, together with the number of entries identified in the NIST NVD, MITRE CVE, and CISA KEV catalog:

Search Term	NIST NVD	MITRE CVE	CISA KEV
CertAgent	0	0	0
Information Security Corporation CertAgent	0	0	174
ISC's Cryptographic Development Kit	0	0	237
ISC CDK DRBG	0	0	195
ISC CDK	0	0	195
Apache Tomcat 9.0.84	0	0	46
Dhuma	0	0	0

For the TOE components, potential vulnerabilities were identified in the CISA KEV catalog only for the search terms "Information Security Corporation CertAgent", "ISC's Cryptographic Development Kit", "ISC CDK DRBG", and "ISC CDK". ISC reviewed the identified entries and determined that none of the reported vulnerabilities apply to the TOE components, including CertAgent, the ISC's Cryptographic Development Kit (CDK), or the ISC CDK DRBG.

Using the search term "Apache Tomcat 9.0.84", ISC identified 46 potential vulnerabilities in the CISA KEV catalog. None of the reported vulnerabilities apply to Apache Tomcat 9.0.119 used in the changed TOE. A detailed analysis of the Apache Tomcat vulnerabilities and their applicability to the TOE is provided in Section 0.

Non-TOE Components

The table below lists the search terms used to identify potential vulnerabilities for the non-TOE components used in the evaluated TOE, together with the number of entries identified in the NIST NVD, MITRE CVE, and CISA KEV catalog:

Search Term	NIST NVD	MITRE CVE	CISA KEV
information security corporation	3	4	176
JDK 17.0.12	4	4	1
Oracle Java 17.0.12	5	5	81
Thales TCT T-5000 Luna Network HSM model VBD-T7 firmware version 7.11.1	0	0	162
Thales TCT T-5000 Luna Network HSM model VBD-T7	0	0	130
HyperSQL	1	2	0
PostgreSQL 15.7	1	1	6
PostgreSQL postgresql_jdbc_driver	0	0	1
RedHat Enterprise 9.2	0	0	14
Windows Server 2019	86	4626	495

The table below lists the additional search terms used to identify potential vulnerabilities for updated non-TOE components used in the changed TOE, together with the number of entries identified in the NIST NVD, MITRE CVE, and CISA KEV catalog:

Addition Search Term	NIST NVD	MITRE CVE	CISA KEV
JDK 17.0.20.1	0	0	1
Oracle Java 17.0.20.1	0	0	81
PostgreSQL 15.18	8	8	1

Potential vulnerabilities were identified using the search term “information security corporation”. ISC reviewed the identified entries and determined that none of the reported vulnerabilities apply to ISC (Information Security Corporation) or its TOE components.

Potential vulnerabilities were identified for Oracle Java 17.0.12. Oracle Java is part of the operational environment and is not part of the TOE. For the changed TOE, Oracle Java was updated to version 17.0.20.1 to incorporate the latest security and maintenance updates. Additional searches were performed using the search terms “JDK 17.0.20.1” and “Oracle Java 17.0.20.1” in the NIST NVD, MITRE CVE, and CISA KEV databases. Although potential vulnerabilities were identified, ISC determined that none apply to Oracle Java 17.0.20.1.

Potential vulnerabilities were identified for HyperSQL. ISC determined that none of the reported vulnerabilities apply to HyperSQL version 2.7.2 used in the evaluated TOE or version 2.7.4 used in the changed TOE.

Potential vulnerabilities were identified for PostgreSQL 15.7. ISC determined that the reported vulnerabilities either do not apply to the PostgreSQL database server itself or do not affect PostgreSQL version 15.7 used in the evaluated TOE. Additional searches were performed using the search term “PostgreSQL 15.18” in the NIST NVD, MITRE CVE, and CISA KEV databases. Although potential vulnerabilities were identified, ISC determined that none apply to PostgreSQL version 15.18.

One potential vulnerability was identified using the search term “PostgreSQL postgresql_jdbc_driver”. ISC reviewed the identified entry and determined that it does not apply to PostgreSQL JDBC driver version 42.7.3 used in the evaluated TOE or version 42.7.11 used in the changed TOE.

Potential vulnerabilities were identified using the search term “RedHat Enterprise 9.2”. ISC reviewed the identified entries and determined that none of the reported vulnerabilities apply to Red Hat Enterprise Linux (RHEL) 9.2.

Potential vulnerabilities were identified using the search term “Windows Server 2019”. Windows Server is part of the operational environment and is not part of the TOE. For the changed TOE, all applicable Microsoft security patches and cumulative updates were applied. A subsequent vulnerability review determined that none of the identified vulnerabilities apply to the updated Windows Server 2019 environment.

Apache Tomcat

Apache Tomcat was updated from version 9.0.104 to version 9.0.119 in the changed TOE.

Using the search term “Apache Tomcat 9.0.84”, which was used during the original evaluation, ISC identified 0 potential vulnerabilities in the NIST NVD and MITRE CVE databases, and 45 potential vulnerabilities in the CISA

KEV catalog. ISC determined that none of the reported vulnerabilities apply to Apache Tomcat 9.0.104 used in the maintained TOE or Apache Tomcat 9.0.119 used in the changed TOE.

Because version-specific searches may not identify all applicable vulnerabilities, ISC also performed searches using the non-version-specific search term "Apache Tomcat".

- NIST NVD: 286 potential vulnerabilities were identified. Of these, 38 apply to Apache Tomcat 9.0.104, and 3 apply to Apache Tomcat 9.0.119.
- MITRE CVE: 323 potential vulnerabilities were identified. Of these, 38 apply to Apache Tomcat 9.0.104, and 3 apply to Apache Tomcat 9.0.119.
- CISA KEV: 45 potential vulnerabilities were identified. ISC determined that none of them apply to Apache Tomcat 9.0.104 or 9.0.119.

The table below lists each identified vulnerability (CVE) from the NIST NVD, MITRE CVE, and CISA KEV databases that applies to Apache Tomcat 9.0.104 or 9.0.119, together with the affected Apache Tomcat version, ISC's applicability assessment for the TOE, and the Tomcat version in which the vulnerability was addressed:

CVE	NIST NVD	MITRE CVE	CISA KEV	Affected Version	Analysis	Fixed in Version
CVE-2026-66713	X	X		9.0.104 9.0.119	Not applicable. Tomcat does not include the WebSocket chat example	9.0.121
CVE-2026-59084	X	X		9.0.104 9.0.119	Not applicable. Tomcat is not configured to use EncryptInterceptor	9.0.120
CVE-2026-59083	X	X		9.0.104 9.0.119	Not applicable. Tomcat is not configured to use rewrite valve	9.0.120
CVE-2026-55956	X	X		9.0.104	Not applicable. Tomcat is not configured to use security constraints	9.0.119
CVE-2026-55955	X	X		9.0.104	Not applicable. Tomcat is not configured to use EncryptInterceptor	9.0.119
CVE-2026-55276	X	X		9.0.104	Not applicable. Tomcat is not configured to use any special roles or authorization constraints	9.0.119

CVE-2026-53434	X	X		9.0.104	Not applicable. Tomcat is not configured to use FFM connector	9.0.119
CVE-2026-53404	X	X		9.0.104	Not applicable. Tomcat is not configured to use rewrite valve	9.0.119
CVE-2026-50229	X	X		9.0.104	Not applicable. Tomcat does not include the number guess example	9.0.119
CVE-2026-43515	X	X		9.0.104	Not applicable. Tomcat is not configured to use security constraints	9.0.118
CVE-2026-43514	X	X		9.0.104	Not applicable. Tomcat is not configured to use AJP protocol	9.0.118
CVE-2026-43513	X	X		9.0.104	Not applicable. Tomcat is not configured to use LockOutRealm	9.0.118
CVE-2026-43512	X	X		9.0.104	Not applicable. Tomcat is not configured to use digest authenticator	9.0.118
CVE-2026-42498	X	X		9.0.104	Not applicable. Tomcat is not configured to accept WebSocket requests	9.0.118
CVE-2026-41293	X	X		9.0.104	Not applicable. Tomcat is not configured to use HTTP/2	9.0.118
CVE-2026-41284	X	X		9.0.104	Not applicable. Tomcat is not configured to accept WebDAV requests	9.0.118
CVE-2026-34500	X	X		9.0.104	Not applicable. Tomcat is not configured to use OCSP checking	9.0.117
CVE-2026-34487	X	X		9.0.104	Not applicable. Tomcat is not configured to use cluster	9.0.117
CVE-2026-34483	X	X		9.0.104	Not applicable. Tomcat is not configured to use JSON access logs	9.0.117

CVE-2026-29146	X	X		9.0.104	Not applicable. Tomcat is not configured to use EncryptInterceptor	9.0.116
CVE-2026-29145	X	X		9.0.104	Not applicable. Tomcat is not configured to use OCSP checking	9.0.116
CVE-2026-25854	X	X		9.0.104	Not applicable. Tomcat is not configured to use cluster	9.0.116
CVE-2026-24880	X	X		9.0.104	Not applicable. Tomcat is not configured to use with a reverse proxy	9.0.116
CVE-2026-24734	X	X		9.0.104	Not applicable. Tomcat is not configured to use an OCSP responder.	9.0.115
CVE-2026-24733	X	X		9.0.104	Not applicable. Tomcat is not configured to have a security constraint to allow HEAD requests to a URI but deny GET requests.	9.0.113
CVE-2025-66614	X	X		9.0.104	Not applicable. Tomcat is not configured with more than one virtual host.	9.0.113
CVE-2025-61795	X	X		9.0.104	Not applicable: The TOE does not use the built-in multipart upload function	9.0.110
CVE-2025-55754	X	X		9.0.104	Not applicable: The TOE does not run Tomcat in a console on Windows	9.0.109
CVE-2025-55752	X	X		9.0.104	Not applicable: The TOE is not configured to use the rewrite valve	9.0.109
CVE-2025-55668	X	X		9.0.104	Not applicable: The TOE is not configured to use the rewrite valve	9.0.106
CVE-2025-53506	X	X		9.0.104	Not applicable: The TOE is not configured to use HTTP/2	9.0.107

CVE-2025-52520	X	X		9.0.104	Not applicable: The TOE doesn't use the built-in multipart upload function	9.0.107
CVE-2025-52434	X	X		9.0.104	Not applicable: The TOE is not configured to use the APR/Native connector	9.0.107
CVE-2025-49125	X	X		9.0.104	Not applicable: The TOE is not configured to use the PreResources or PostResources mounted function	9.0.106
CVE-2025-49124	X	X		9.0.104	Not applicable: The TOE does not use the built-in Tomcat installer for Windows	9.0.106
CVE-2025-48989	X	X		9.0.104	Not applicable: The TOE is not configured to use HTTP/2	9.0.108
CVE-2025-48988	X	X		9.0.104	Not applicable: The TOE doesn't use the built-in multipart upload function	9.0.106
CVE-2025-46701	X	X		9.0.104	Not applicable: The TOE is not configured to use the GCI servlet	9.0.105

Although 38 vulnerabilities were identified for Apache Tomcat versions 9.0.104 and 9.0.119, ISC determined that none are applicable to the maintained or changed TOE due to the TOE's configuration, disabled functionality, or non-use of the affected components.

Of these 38 vulnerabilities, 35 have been addressed in Apache Tomcat 9.0.119, which is used in the changed TOE. The remaining 3 vulnerabilities, CVE-2026-59084 and CVE-2026-59083, addressed in Apache Tomcat 9.0.120, and CVE-2026-66299, addressed in Apache Tomcat 9.0.121, have not been addressed in the Apache Tomcat 9.0.119 included in the changed TOE. However, ISC determined that none of these vulnerabilities apply to either the maintained TOE or the changed TOE.

Apache Log4j

Apache Log4j was updated from version 2.22.0 to version 2.26.0 in the changed TOE. ISC performed vulnerability searches using the search term "Apache Log4j".

NIST NVD: 23 potential vulnerabilities were identified. Of these, 6 apply to Apache Log4j 2.22.0, and 2 apply to Apache Log4j 2.26.0.

- MITRE CVE: 34 potential vulnerabilities were identified. Of these, 6 apply to Apache Log4j 2.22.0, and 2 apply to Apache Log4j 2.26.0.
- CISA KEV: 44 potential vulnerabilities were identified. ISC determined that none of the identified vulnerabilities apply to Apache Log4j 2.22.0 or 2.26.0.

The table below lists each identified vulnerability (CVE) from NIST NVD, MITRE CVE, and CISA KEV databases that applies to Apache Log4j 2.22.0 or 2.26.0, together with the affected Apache Log4j version, ISC's applicability assessment for the TOE, and the Apache Log4j version in which the vulnerability was addressed:

CVE	NIST NVD	MITRE CVE	CISA KEV	Affected Version	Analysis	Fixed in Version
CVE-2026-49844	X	X		2.22.0 2.26.0	Not applicable. The TOE is not configured to use JSON template layout	2.26.1
CVE-2026-34481	X	X		2.22.0 2.26.0	Not applicable. The TOE is not configured to use JSON template layout	2.26.1
CVE-2026-34480	X	X		2.22.0	Not applicable. The TOE is not configured to use XML layout	2.25.4
CVE-2026-34478	X	X		2.22.0	Not applicable. The TOE is not configured to use RFC 5424 layout	2.25.4
CVE-2026-34477	X	X		2.22.0	Not applicable. The TOE is not configured to use Network appender	2.25.4
CVE-2025-68161	X	X		2.22.0	Not applicable. The TOE is not configured to use Network appender	2.25.3

Although 6 vulnerabilities were identified for Apache Log4j 2.22.0 and 2 for Apache Log4j 2.26.0, ISC determined that none are applicable to the maintained or changed TOE because the affected functionality is not used by the TOE.

Of the 6 vulnerabilities applicable to Apache Log4j 2.22.0, 4 have been addressed in Apache Log4j 2.26.0 used in the changed TOE. The remaining 2 vulnerabilities (CVE-2026-49844 and CVE-2026-34481) were addressed in Apache Log4j 2.26.1, which is not included in the changed TOE. However, ISC determined that neither vulnerability applies to the maintained nor changed TOE.

Other Libraries

ISC performed a vulnerability assessment of the third-party libraries included in the TOE that have not changed since the validated TOE: com.google.code.gson 2.10.1, jQuery 3.7.1, and jQuery UI 1.13.2. The following search terms were used in the NIST NVD, MITRE CVE, and CISA KEV databases:

- com.google.code.gson
- jQuery 3
- jQuery UI

ISC reviewed the identified CVEs and determined that none are applicable to the validated, maintained, or changed TOE.

Conclusion

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. The changes do not introduce or modify any TSF interfaces, do not affect any SFRs, and do not alter the TOE's security functionality. No new assurance activities are required.

The regression and targeted testing performed by ISC covered all changes, all TSF interfaces and SFRs that could reasonably be affected by those changes, and the majority of the remaining SFRs. The successful test results demonstrate that the changed TOE continues to satisfy the requirements of the Protection Profile (PP).

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