ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
Information Security Corporation CertAgent/Dhuma v8.0 patch level 0.3

Maintenance Update of Information Security Corporation CertAgent/Dhuma v8.0 patch level 0.2

Maintenance Report Number: CCEVS-VR-VID11457-2024

Date of Activity: 2 December 2024

References:

1. Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008.
2. Information Security Corporation CertAgent/Dhuma Impact Analysis Report for Common Criteria Assurance Maintenance Update from Version 8.0, Patch Level 0.2 to Version 8.0, Patch Level 0.3, 1 November 2024.
3. Protection Profile for Certification Authorities, version 2.1 [PP_CA_V2.1]

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: CertAgent/Dhuma v8.0 patch level 0.2 Security Target for Common Criteria Evaluation, version 5.0.12, August 23, 2024	**Maintained Security Target:** CertAgent/Dhuma v8.0 patch level 0.3 Guidance for Common Criteria Evaluation, version 3.0.6, September 9, 2024.

Guidance for Common Criteria Evaluation: CertAgent/Dhuma v8.0 patch level 0.2 Guidance for Common Criteria Evaluation, version 3.0.5, July 25, 2024	**Maintained Guidance for Common Criteria Evaluation:** CertAgent/Dhuma v8.0 patch level 0.3 Guidance for Common Criteria Evaluation, version 3.0.6, September 9, 2024
Common Criteria Security Target: CertAgent/Dhuma v8.0 patch level 0.2 Security Target for Common Criteria Evaluation, version 5.0.12, August 23, 2024	**Maintained Common Criteria Security Target:** CertAgent/Dhuma v8.0 patch level 0.3 Security Target for Common Criteria Evaluation, version 5.0.13, September 9, 2024
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., March 7, 2024.	**Maintained Administrator Guide:** CertAgent/Dhuma Administrator Guide, version 8.0, July 22, 2024
Certificate Authority Guide: CertAgent Certificate Authority Guide, version 8.0, July 22, 2024	**Maintained Certificate Authority Guide:** CertAgent Certificate Authority Guide, version 8.0, July 22, 2024
Public Site Guide: CertAgent Public Site Guide, version 8.0, March 7, 2024	**Maintained Public Site Guide:** CertAgent Public Site Guide, version 8.0, July 22, 2024
Release Notes: CertAgent/Dhuma Release Notes, version 8.0.0.2, March 22, 2024	**Maintained Release Notes:** CertAgent/Dhuma Release Notes, version 8.0.0.3, July 29, 2024

Assurance Continuity Maintenance Report:

Information Security Corporation submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 1 November 2024. 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 Assurance Continuity evidence consists of

- CA/Dhuma V8.0 patch level 0.3 Security Target, 1 Nov 2024
- CA/Dhuma V8.0 patch level 0.3 Guidance for CC Evaluation v3.0.6,
- CA/Dhuma V8.0 patch level 0.3 Impact Analysis Report (IAR) 1 Nov 2024
- CA/Dhuma V8.0 patch level0.2 Guidance for CC Evaluation, 25 Jul 2024
- CA/Dhuma V8.0 Administrator Guide, 22 Jul 2024
- CA/Dhuma V8.0 Installation, Configuration, and Management Guide, 30 Jul 2024.
- CA/Dhuma V8.0.0.3 Release Notes, 29 Jul 2024
- CertAgent V8.0 Certificate Authority Guide, 22 Jul 2024Help
- CertAgent V8.0 Public Site Guide, 22 Jul 2024

Changes to the TOE

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 which were made to fix defects or vulnerabilities. ISC has evaluated each change, and 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 changes did not require any updates to the CAVP certificates and the certificates for the original evaluation are considered to be valid for the updated TOE.

For this Assurance Continuity, the version number of the TOE changed from Version 8.0 patch level 0.2 to Version 8.0 patch level 0.3 due to the minor updates made to the TOE. These versions are also known as 8.0.0.2 and 8.0.0.3,

The following changes to the TOE were made to address published vulnerabilities and defects.

Updated Apache Tomcat

Apache Tomcat has been updated from version 9.0.84 to version 9.0.91 to address published vulnerabilities and defects. ISC performed a code review and analysis of the changes using the following resources:

- Apache Tomcat 9 Changelog
  https://tomcat.apache.org/tomcat-9.0-doc/changelog.html
- Apache Tomcat on GitHub
  https://github.com/apache/tomcat

The table below lists the Apache Tomcat versions, changes that were applied to each changed TOE, and ISC's analysis of the change.

Version	Change	Analysis
9.0.85	Relax the check that the HTTP Host header is consistent with the host used in the request line, if any, to make the check case insensitive since host names are case insensitive. (markt)	Minor. Bug fix.
9.0.86	Review usage of debug logging and downgrade trace or data dumping operations from debug level to trace. (remm)	Minor. Updated debug/trace messages.
	Further improve the performance of request attribute access for ApplicationHttpRequest andApplicationRequest. (markt)	Minor. Code improvement.
	Partial fix for 68558: Cache the result of converting to String for request URI, HTTP header names and the request Content-Type value to improve performance by reducing repeated byte[] to String conversions. (markt)	Minor. Code improvement.

	68546: Generate optimal size and types for JSP imports maps, as suggested by John Engebretson	Minor. Code improvement
	Add strings for debug level messages.	Minor. Added debug messages.
9.0.87	Minor performance improvement for building filter chains. Based on ideas from pull request #702 by Luke Miao. (remm)	Minor. Code improvement.
	Align error handling for Writer and OutputStream. Ensure use of either once the response has been recycled triggers a NullPointerException provided that discardFacades is configured with the default value of true. (markt)	Minor. Bug fix.
9.0.88	Add checking of the "age" of the running Tomcat instance since its build-date to the SecurityListener, and log a warning if the server is old. (schultz)	Minor. Added a warning message.
	Change the thread-safety mechanism for protecting StandardServer.services from a simple synchronized lock to a ReentrantReadWriteLock to allow multiple readers to operate simultaneously. Based upon a suggestion by Markus Wolfe.	Minor. Code improvement.
	Improve Service connectors, Container children and Service executors access sync using a ReentrantReadWriteLock. (remm)	Minor. Code improvement.
	Improve handling of integer overflow if an attempt is made to upload a file via the Servlet API and the file is larger than Integer.MAX_VALUE. (markt)	Minor. Bug fix.
	68862: Handle possible response commit when processing read errors. (remm)	Minor. Bug fix.
	Add threadsMaxIdleTime attribute to the endpoint, to allow configuring the amount of time before an internal executor will scale back to the configured minSpareThreads size. (remm)	Minor. Code improvement.
	Handle the case where the JSP engine forwards a request/response to a Servlet that uses an OutputStream rather than a Writer. This was triggering an IllegalStateException on code paths where there was a subsequent attempt to obtain a Writer. (markt)	Minor. Bug fix.
9.0.89	Deprecate and remove sessionCounter (replaced by the addition of the active session count and the expired session count, as a reasonable approximation) and duplicates (which does not represent a possible event in current implementations) statistics from the session manager. (remm)	Minor. Code improvement.

	Extend Asn1Parser to parse UTF8Strings	Minor. Added UTF8String parsing.
	Align non-secure and secure writes with NIO and skip the write attempt when there are no bytes to be written. (markt)	Minor. Code improvement.
	Allow any positive value for socket.unlockTimeout. If a negative or zero value is configured, the default of 250ms will be used. (mark)	Minor. Changed the default from 2s to 250ms and allowed any positive value rather than 2s or above.
	Reduce the time spent waiting for the connector to unlock. The previous default of 10s was noticeably too long for cases where the unlock has failed. The wait time is now 100ms plus twice socket.unlockTimeout. (markt)	Minor. Changed the default configuration.
	Ensure that the onAllDataRead() event is triggered when the request body uses chunked encoding and is read using non-blocking IO. (markt)	Minor. Bug fix.
	68934: Add debug logging in the latch object when exceeding maxConnections. (remm)	Minor. Added debug messages.
	Refactor trailer field handling to use a MimeHeaders instance to store trailer fields. (markt)	Minor. Code improvement.
	Ensure that multiple instances of the same trailer field are handled correctly. (markt)	Minor. Bug fix.
	Fix non-blocking reads of chunked request bodies. (markt)	Minor. Bug fix.
	When an invalid HTTP response header was dropped, an off-by-one error meant that the first header in the response was also dropped. Fix based on pull request #710 by foremans. (markt)	Minor. Bug fix.
	Switch to using the Base64 encoder and decoder provided by the JRE rather than the version provided by Commons Codec. The internal fork of Commons Codec has been deprecated and will be removed in Tomcat 11. (markt)	Minor. Code updated. Used JRE's built in base64 encoder and decoder.
9.0.90	The system property org.apache.catalina.connector.RECYCLE_FACADES will now default to true if not specified, which will in turn set the default value for the discardFacades connector attribute, thus causing facade objects to be discarded by default. (remm)	Minor. Changed the default setting. Facade objects are now discarded rather than reused by default.

	69133: Add task queue size configuration on the Connector element, similar to the Executor element, for consistency. (remm)	Minor. Added a configuration.
	68546: Small additional optimisation for initial loading of Servlet code generated for JSPs. Based on a suggestion by Dan Armstrong. (markt)	Minor. Code improvement.
9**.0.91**	Improve the algorithm used to identify the IP address to use to unlock the acceptor thread when a Connector is listening on all local addresses. Interfaces that are configured for point to point connections or are not currently up are now skipped. (markt)	Minor. Code improvement.
	Following the trailer header field refactoring, -1 is no longer an allowed value for maxTrailerSize. Adjust documentation accordingly. (remm)	Minor. Updated document.
	Update the optimisation in jakarta.el.ImportHandler so it is aware of new classes added to the java.lang package in Java 23. (markt)	Minor. Bug fix.
	Ensure that an exception in toString() still results in an ELException when an object is coerced to a String using ExpressionFactory.coerceToType(). (markt)	Minor. Bug fix.

These changes do not affect any TSF interfaces, SFRs, or security functions. The following SFRs or SARs are associated with this change: FCS_TLSS_EXT.1, FCS_TLSS_EXT.2, FCS_HTTPS_EXT.1, FTP_ITC.1, FTP_TRP.1, FAU_GEN.1, FDP_OCSPG_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_UAU_EXT.1, FIA_UIA_EXT.1, FIA_ESTS_EXT.1, FMT_SMR.2 and FTA_SSL.3, FTA_SSL.4. ISC rates the impact on assurance as minor because after a review of the Apache Tomcat Changelog and code (as detailed above) we concluded that there were only minor changes in functionality used by the TOE.

Development Environment

There have been no changes to the development environment.

Affected Developer Evidence

The AGD document named “CertAgent/Dhuma Guidance for Common Criteria Evaluation” has been updated to version 3.0.6, September 9, 2024.
The Security Target document named “CertAgent/Dhuma Security Target for Common Criteria Evaluation” has been updated to version 5.0.13, September 9, 2024.
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 sections below describe the components that caused the developer evidence to be updated.

NOTE: Only some of the TOE changes required updated evidence. Some of the changes that are not part of the TOE evaluation, or do not require any assurance activities, are not listed.

Installation Changed

The installation includes the updated TOE version number (8.0.0.3) and an updated version of Apache Tomcat (9.0.91).
Guidance document sections 1.2.1, 1.2.2, 2.7, 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.

Assurance Documents Changed

The AGD document named "CertAgent/Dhuma Guidance for Common Criteria Evaluation" has been updated to version 3.0.6, September 9, 2024.
CertAgent/Dhuma Security Target for Common Criteria Evaluation has been updated to version 5.0.13, September 9, 2024.

Description of Regression Testing

Regression and new feature 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 TOE. All tests passed.

Test Details

Changes Testing

Updated Apache Tomcat

The Tomcat update was tested by ISC by performing the tests in 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, and FTA_SSL.4 User-Initiated Termination and verifying the results.

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.

Assurance Activity Coverage Argument

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

Vulnerability Coverage Argument

On November 1, 2024 ISC performed a vulnerability assessment on the libraries used by the validated and changed TOE, using the following resources:

- NIST Vulnerability Database
  https://nvd.nist.gov/vuln/search
- Apache Tomcat 9.x vulnerabilities:
  https://tomcat.apache.org/security-9.html

Apache Tomcat

Apache Tomcat changed from version 9.0.84 to 9.0.91 in the TOE.
"Apache Tomcat 9" search term was used in the NIST National Vulnerability Database (https://nvd.nist.gov/vuln/search) and found 76 potential vulnerabilities. Among the 76 vulnerabilities, only 3 of them applied to Apache Tomcat 9.0.84 (used in the validated TOE) and none of them applied to Apache Tomcat 9.0.91 (used in the changed TOE). 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-2024-34750	Not applicable: The TOE is not configured to use HTTP/2	9.0.90
CVE-2024-24549	Not applicable: The TOE is not configured to use HTTP/2	9.0.86
CVE-2024-23672	Not applicable: The TOE doesn't support WebSocket	9.0.86

Among the 3 vulnerabilities found in version 9.0.84, none of them applied to the validated TOE. All of the vulnerabilities have been addressed in the changed TOE.

Other Libraries

ISC performed a vulnerability assessment on the libraries that have not been changed since the maintained TOE and found a total of thirty two (32) potential vulnerabilities using the database search functionality of NIST National Vulnerability Database (https://nvd.nist.gov/vuln/search). The table below lists each potential vulnerability identified and its applicability to the TOE. None

of the vulnerabilities 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		Not applicable: doesn't apply to the jQuery 3.7.1 library used by the TOE
CVE-2020-11023		

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		

Conclusion

TOE changed from Version 8.0 patch level 0.2 to Version 8.0 patch level 0.3. The changes to the product fixed defects or vulnerabilities identified in the Apache Tomcat Server which was updated from version 9.0.84 to version 9.0.91 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 requirements in the PP and the changes were minor enough to not manifest at the level required to perform any specific test assurance activity. The changes made to the Apache Tomcat Server resulted in the version update to the TOE and its associated documentation which is a minor change. We conclude that the assurance impact is minor.