ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Tripwire, Inc. Tripwire Enterprise Version 8.3 with the 8.3.5 patch

Maintenance Update of Tripwire, Inc. Tripwire Enterprise Version 8.3 with the 8.3.5 patch

Maintenance Report Number: CCEVS-VR-VID10462-2014

Date of Activity: 20 October 2014

References: Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004;

Tripwire Enterprise Version 8.3 Impact Analysis Report, Version 1.2, 10/19/2014

Documentation Updated: (List all documentation updated)

- Security Target: Tripwire, Inc. Tripwire Enterprise Version 8.3 Security Target, Version 1.2, 10/19/2014
- Design Documentation: Tripwire, Inc. Tripwire Enterprise Version 8.3 Design Document, Version 1.0, October 1, 2014
- Test Plan: No changes required. Note that regression testing was performed by the vendor before the major release with appropriate regression testing for the patch.
- Lifecycle:

  Tripwire, Inc. Tripwire Enterprise Version 8.3 Configuration Management Plan, Version 1.2, October 19, 2014

  Tripwire, Inc. Tripwire Enterprise Version 8.3 Delivery Procedures, Version 1.0, October 1, 2014
- Tripwire, Inc. Tripwire Enterprise Version 8.3 Life Cycle Document, Version 1.0, September 30, 2014
- Administrative Guidance:

  Tripwire Enterprise Version 8.3 User Guide

  Tripwire Enterprise Version 8.3 Reference Guide

  Tripwire Enterprise Version 8.3 Installation & Maintenance Guide

  Installing TE Console on Microsoft Windows Server 2012

  Tripwire Enterprise v8.3 Supplemental Common Criteria Guidance, Version 1.0, Release Date October 1, 2014

Assurance Continuity Maintenance Report:

The vendor (Tripwire Inc.) for the Tripwire Enterprise Product (originally evaluated at Version 8.1 with the 8.1.2.5 patch) submitted an Impact Analysis Report (IAR) to bring the product to Version 8.3 with the 8.3.5 patch to CCEVS for approval on 19 October 2014. The IAR was intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version

1.0, February 2004. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

Changes to TOE:

The TOE is Tripwire Enterprise Version 8.3 (TE v8.3) with the 8.3.5 patch, provided by Tripwire, Inc. The TOE type is an intrusion detection system consisting of a sensor, scanner, and analyzer to monitor IT systems for activity that may indicate inappropriate activity on the IT system. The server portion of the TOE is a software-only TOE that runs on the Windows, Solaris, SuSE and Red Hat Enterprise Linux operating systems. The Agent portion of the TOE can be installed and executed on the operating systems identified in the ST. TE v8.3 performs file-integrity monitoring, change auditing, configuration assessment, and compliance reporting. The TOE is an attribute change assessment product that also reconciles the changes against existing management systems and policies.
The TOE consists of a server application component (Tripwire Enterprise Server), a client application component (Tripwire Enterprise Agent), and a client administrative console application component (Tripwire CLI). The product requires a database application to support the product's storage needs (MySQL is bundled with TE v8.3). Since TE v8.3 supports the ability to operate with a database from differing vendors (as identified in Section 1.4.2.1), the database is considered part of the operational environment. The product supports two different installation configurations and both are allowed in the evaluated configuration. With a single system installation, the TE Server and database are installed on the same system. With a distributed installation, TE Server and database are installed on different systems. In the CC evaluated configuration, the TE Server must be configured to encrypt all communications between the TE Server and the database, or the database must reside on the same system as the TE server, or the database must reside on a system located on a private physical network that is not globally routable and is protected from attacks and from unauthorized physical access. The other TOE components can run on different machines in various combinations.

The TOE was revised in the following ways, with examples given of each type of change. A full list of changes may be found in the impact analysis report. This IAR covered a total of 126 changes to the product.

1. **Bug Fixes** (42 changes): Changes to the validated TOE to correct a bug that do not affect the assurance evidence or changed the evaluated security policy. Examples:
    - Resolving various reported issues for edge scenarios to make TOE behave as described in the documentation.
2. **Documentation** (3 changes): Changes to the guidance to clarify installation and usage of product features. No changes were made to the security configuration. Examples:
    - Additional installation instructions
    - Fixed broken documentation links
3. **Not Security Relevant** (36 changes): Changes to or the addition of non-security relevant functionality. Examples:
    - New health checks
    - Additional asset classifications
    - Enhanced Data API
    - Additional error logging
4. **Environmental** (6 changes): Changes to the IT environment that do not affect the validated TOE. Examples:
    - New Agent platforms
    - New Console platforms
    - Support for newer versions of Java

5. **Not In TOE** (17 changes): Changes to the product that are not part of the evaluated TOE / TSF. Examples:
    - New importable rulesets (only rule primitives were covered, not predefined rulesets)
    - New configurator interface (excluded from TOE)
    - Fix to support stronger certificates in IE8 (IE8 is not a TOE-approved browser)
    - Changes in SCAP support (SCAP is excluded from TOE)
    - Updated rule tests with new capabilities that were explicitly excluded from the TOE
6. **Performance** (7 changes): Performance enhancements (changes to or addition of non-security relevant functionality). Examples:
    - Improved speed of cache regeneration
    - Improved performance when rescoring results
7. **Enhancements** (15 changes): Changes to the product to strengthen security and enhance validated security features. These changes do not add new security policies, nor do they change the SFRs. There may be additional implementation detail in the TSS of the ST. Examples:
    - Enhanced password complexity (all existing capabilities in the SFR maintained; new capabilities described in TSS and tested)
    - Console enhancements to prevent various potential attacks
    - Enhanced security checks internally to protect TOE (below the level of the TSS)
    - Increased the number of comparisons in policy tests (below the level of TSS description)

The evaluation evidence consists of the Security Target, updated manuals, administrative guidance, design documents, life cycle documents, and test evidence. The documentation was updated as follows:

- Security Target: Tripwire, Inc. Tripwire Enterprise Version 8.3 Security Target, Version 1.2, 10/19/2014
    - Updated unique TOE identifier and dates
    - Updated software products in the operating environment to be later versions
    - Described enhanced password complexity implementation
    - Identified additional tools excluded from the TOE
    - Indicated monitoring DACL and SACL elements were outside the TOE
- Design Documentation: Tripwire, Inc. Tripwire Enterprise Version 8.3 Design Document, Version 1.0, October 1, 2014
    - Updated unique TOE identifier, dates, and references
    - Described enhanced password complexity implementation
    - Added new SOAP interfaces (setName, configureNodeEventGenerator, newUser)
    - Added REST API description
    - Added description of Configurator with an explanation that it is not in the TOE
- Test Plan: No changes required. Note that regression testing was performed by the vendor before the major release with appropriate regression testing for the patch.
- Lifecycle:

  Tripwire, Inc. Tripwire Enterprise Version 8.3 Configuration Management Plan, Version 1.2, October 19, 2014

- Updated unique TOE identifier and dates
- Updated software products in the operating environment to be more recent versions
- Updated 8.3.5 3rd party library supplier list
- Updated unique configuration item identifiers

Tripwire, Inc. Tripwire Enterprise Version 8.3 Delivery Procedures, Version 1.0, October 1, 2014

- Updated TOE identifier

- Tripwire, Inc. Tripwire Enterprise Version 8.3 Life Cycle Document, Version 1.0, September 30, 2014
  - Updated unique TOE identifier and dates
  - Updated description of physical security for the development lab, including a change from key fobs to smart cards.
  - Updated to indicate that Tripwire sometimes completes background checks
- Vulnerability Analysis: No changes required.
- Administrative Guidance:

  Tripwire Enterprise Version 8.3 User Guide

  Tripwire Enterprise Version 8.3 Reference Guide

  Tripwire Enterprise Version 8.3 Installation & Maintenance Guide

  Installing TE Console on Microsoft Windows Server 2012

  - Changes were made to the documents above to correct or clarify information, as well as to describe changes to the graphical user interface to make it easier to use. In addition, these guides may describe new or modified features that are outside the evaluated configuration as indicated in the Supplemental Guidance.

  Tripwire Enterprise v8.3 Supplemental Common Criteria Guidance, Version 1.0, Release Date October 1, 2014

  - Identified SCAP and DSR as outside the scope of the evaluation.
  - Updated the TE Server platforms list.
  - Updated the TE Agents platforms lists.
  - Updated the list of databases, virtual environments, directory services, network devices on which TE can monitor.
  - Updated password guidelines section to reflect the new password complexity implementation.

The TOE has no known outstanding security-related vulnerabilities at this time. The vendor performed regression testing as part of the major release, and reran selected portions of the regression testing for the 8.3.5. New features were tested as part of normal product testing; this was acceptable as these features did not correspond to new or changed SFRs. There were no additional issues.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and concur with the IAR's assessment that the changes are minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.