National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Tripwire Manager, version 4.6.1 with Tripwire for Servers, version 4.6.1

Report Number:	**CCEVS-VR-VID10124-2009**
Dated:	**29 June 2009**
Version:	**1.3**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Scott Shorter, Orion Security Solutions
Daniel P. Faigin, The Aerospace Corporation

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of Tripwire Manager, version 4.6.1 with Tripwire for Servers, version 4.6.1 was performed by SAIC, in the United States and was completed in May 2009. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Tripwire TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3 and International Interpretations effective on 30, September 2006. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.2.

Science Applications International Corporation (SAIC) determined that the evaluation assurance level (EAL) for the product is EAL 3 family of assurance requirements augmented with ALC_FLR.2. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Tripwire, Inc. Tripwire Manager, version 4.6.1 with Tripwire for Servers, version 4.6.1 Security Target.

This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Tripwire product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, examined evaluation testing procedures, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The validation team notes that the claims made and successfully evaluated for the product represent a more limited set of requirements than what might be used for a "normal" product deployment. Specifically, no claims are made for protection of data transmission between parts of the TOE in spite of the fact that it will mostly likely be configured and setup in a distributed fashion over a network whose traffic could well be less than benign. It then becomes quite necessary for the administrators to fulfill the requirements levied on the environment

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The technical information included in this report was obtained from the Evaluation Technical Report for Tripwire Manager, version 4.6.1 with Tripwire for Servers, version 4.6.1 (ETR) Parts I and II produced by SAIC.

1.1 Evaluation Details

Evaluated Product:	Tripwire Manager, version 4.6.1 with Tripwire for Servers, version 4.6.1

Security Target:	Tripwire, Inc. Tripwire Manager, Version 4.6.1, with Tripwire for Servers, Version 4.6.1 Security Target, Version 1.0, 1 May, 2009
Sponsor & Developer:	Tripwire, Inc 101 SW Main Street, Suite 1500 Portland, OR 97204
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Completion Date:	May 2009
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation, Version 2.3
Evaluation Class:	EAL 3 augmented with ALC_FLR.2
Description	The TOE is a change audit assessment product that can assure the integrity of critical data on system(s) by monitoring file system object attributes for unauthorized or unexpected modification. The TOE accomplishes this by detecting the corrupted or altered files and reporting the occurrence to the system administrators, so corrective actions can be taken. The TOE can monitor the attributes of UNIX files, Windows files, and Windows Registry keys for unauthorized or unexpected modification. The TOE is designed to monitor servers in general. It can monitor servers that run on either Windows or several types of UNIX operating systems. The TOE does not interact with the server as a server but as a program running on an operating system. The TOE administrator configures the server objects to be monitored but the TOE does not provide general user services.
Disclaimer	The information contained in this Validation Report is not an endorsement of the Tripwire product by any agency of the U.S. Government and no warranty is either expressed or implied.
PP:	none
Evaluation Personnel	Shukrat Abbas Quang Trinh
Validation Team:	Scott Shorter, Orion Security Solutions Daniel P. Faigin, The Aerospace Corporation

1.2 Interpretations

The Evaluation Team determined that there were no NIAP Interpretations applicable to this evaluation:

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

- An authorized user may incorrectly change TOE data or functions they are authorized to modify.
- An attacker may be able to inappropriately change attribute information for targeted objects and have that change go undetected.
- An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
- An attacker may be able to gain unauthorized access to data collected from targeted objects.

2 Identification

The product being evaluated is Tripwire Manager, version 4.6.1 with Tripwire for Servers, version 4.6.1. The TOE is configured in accordance to the Release Notes, installation and user guides.

3 Security Policy

There are no explicit Security Policies for the evaluated product, but it does implement a number of security features:

- **Change Audit Assessment**: Tripwire Manager with Tripwire for Servers can assure the integrity of critical data on system(s) by monitoring file system object attributes for unauthorized or unexpected modification. Note that the TOE can use the SNMP or email servers provided by the IT Environment to send alert messages. The TOE is also dependent upon its environment, e.g., UNIX *crontab*, in order to schedule periodic change audits.
- **Security Audit:** Tripwire Manager with Tripwire for Servers generates audit records of the management actions that occur on the TOE. Note that the audit trail is stored in and protected by the IT environment.
- **Cryptographic Support:** Tripwire Manager with Tripwire for Servers digitally signs stored attribute baselines for objects, as well as configuration files and reports written to files. The TOE also uses SSL to protect communication between its components.
- **Identification and Authentication:** Tripwire Manager with Tripwire for Servers requires that users are authenticated using a passphrase before any access to the TOE and the TOE security-relevant data is allowed. Note that the only logon into the TOE is an administrator role logon -- individual users are not identified the TOE.
- **Security Management:** Tripwire Manager with Tripwire for Servers provides administrator console interface used by authorized administrators to manage the TOE, and its functions.
- **Protection of the TSF**: Tripwire Manager with Tripwire for Servers uses SSL to protect the communication between TOE components. Note that the Tripwire for Servers

component executes as a trusted process within its host operating system. In Unix based operating systems, the TOE executes as ROOT, while on Windows platforms the TOE executes as a SYSTEM process. Furthermore, the TOE uses features provided by its IT environment to protect itself from external tampering. The TOE utilizes the process mechanism in the IT environment as a protected domain of execution. Also, the TOE uses the abstraction of files and a file protection mechanism (e.g., access control lists) in the IT environment to protect TOE executables, TOE configuration data, and TOE output data. The IT Environment also provides the timestamp used in the audit records.

4 Assumptions

The following assumptions are identified in the Security Target:

4.1 Intended Usage Assumptions

- The TOE has access to all the IT System data it needs to perform its functions.
- The TOE will be configured to monitor products that it is compatible with and in quantities it can handle.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

4.2 Physical Assumptions

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

4.3 Personnel Assumptions

- There will be one or more competent individuals assigned to manage the TOE and its supporting platforms and the security of the information they contain.
- The authorized administrators are not willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE and its supporting platforms documentation.
- The TOE and its supporting platforms can only be accessed by authorized users.

4.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made; and meets them with only a certain level of assurance (EAL 3 augmented with ALC_FLR.2 in this case).
2. As with all EAL 3 evaluations, this evaluation did not specifically search for vulnerabilities that were not “obvious” (as this term is defined in the CC and CEM); seriously attempt to find counters to them; nor find vulnerabilities related to objectives not claimed in the ST.

3. The supporting features provided by the IT environment have not been subject to this evaluation. As such, protections and other functions (such as reliable time) afforded by the operating systems, scheduling capabilities, audit storage and protection, and the supporting SSL mechanism.

5 Architectural Information

The Tripwire Product includes three components: Tripwire for Servers, Tripwire Manager, and Tripwire Utilities. The security relevant portions of the TOE are the Tripwire for Servers and the Tripwire Manager components. The Tripwire Utilities component is part of the TOE but does not enforce any security functions. Both of the security relevant components include a crypto module subcomponent[1].

Authorized administrators configure the TOE by creating integrity check rules that specify objects and corresponding object attributes to monitor. These are stored in a policy file configuration file, thus creating a baseline. After making changes to the baseline the administrator can use the TOE to perform integrity checks at regular intervals using IT Environment support such as *crontab* for example on UNIX operating systems or scheduled checks using TOE interfaces.

The TOE provides its own audit mechanism that can generate audit records containing integrity check results and TOE management actions. The TOE does not maintain its own audit trail however – audit records are sent by the TOE to the underlying operating system audit mechanism to add to its audit trail. Auditing in the TOE is not enabled by default and must be enabled by an authorized administrator in the evaluated configuration.

The TOE provides a non-FIPS validated crypto module that can generate cryptographic keys and can digitally sign/verify, and encrypt/decrypt files when stored in its environment. Files that are encrypted during storage are attribute baselines for objects, configuration and policy files. Files that are signed during storage are attribute baselines for objects and report files. The crypto module can also perform SSL operations to protect communication between TOE components.

The TOE provides two sets of interfaces to control how it operates: a Graphical User Interface (GUI) in the Tripwire Manager component and a Command-Line Interface (CLI) in each Tripwire for Servers component. Both interfaces provide the same administrative functions and have the same restrictions. Administrators can either connect to each Tripwire for Server component and administer it with its CLI or connect to the Tripwire Manager and use its GUI to administer multiple Tripwire for Server components.

The TOE in its intended environment consists of the following components:

- Tripwire for Servers component – Monitors the object attributes of file system objects for unauthorized or unexpected modification. The set of objects monitored is configurable, but are generally those objects that are critical to the secure operation of the particular server that the TOE is protecting. These may be objects generated by the host operating system or objects generated by the server application. There is a UNIX version of this component as well as a Windows version of this component. The UNIX version is used to monitor UNIX files. The Windows version is used to monitor Windows files and registry keys.
- *twadmin* subcomponent – Used to create and sign the configuration and policy files used by Tripwire for Servers

[1] The developer asserts that correctness of the cryptographic functions provided by the TOE. The cryptographic functions have not been FIPS validated.

- *twprint* subcomponent – Used for reporting when management is performed locally
- *tripwire* subcomponent – Used for creating a baseline of the target server and for performing integrity checking
- *twagent* subcomponent – Provides a network interface to the above three Tripwire for Servers subcomponents that is accessible using the Tripwire Manager component.
- Tripwire Manager component – Provides graphical user interface (GUI) administrative console that can be used to manage the Tripwire for Servers component.
- Tripwire Utilities – Useful for troubleshooting problems with Tripwire for Servers configuration.

The following the IT environment components that support the TOE:

- Operating system – Provides runtime environment for Tripwire for Servers component and JVM. Also supports TOE audit security function.
- Tripwire For Servers - Solaris 2.6, 7, 8, 9, 10; AIX 5.2, 5.3; Windows NT, 2000, XP Professional, 2003; Red Hat Linux 9.0; Red Hat Enterprise Linux 3.0, 4.0; HP-UX 11, 11i; HP-UX Itanium 11iv2.
- Tripwire Manager - Solaris 7,8, 9; Windows 2000, XP Professional, 2003; Red Hat Linux 9.0; Red Hat Enterprise Linux 3.0, 4.0.
- Java Virtual Machine (JVM) – Provides runtime environment for Tripwire Manager component. - Sun Java 2 JRE v1.4
- Email server – Provides the ability to send alerts generated by the TOE to administrators using email.
- SNMP server – Provides the ability to send alerts generated by the TOE to administrators using SNMPv1.

The TOE in its intended environment is depicted in the figure below.

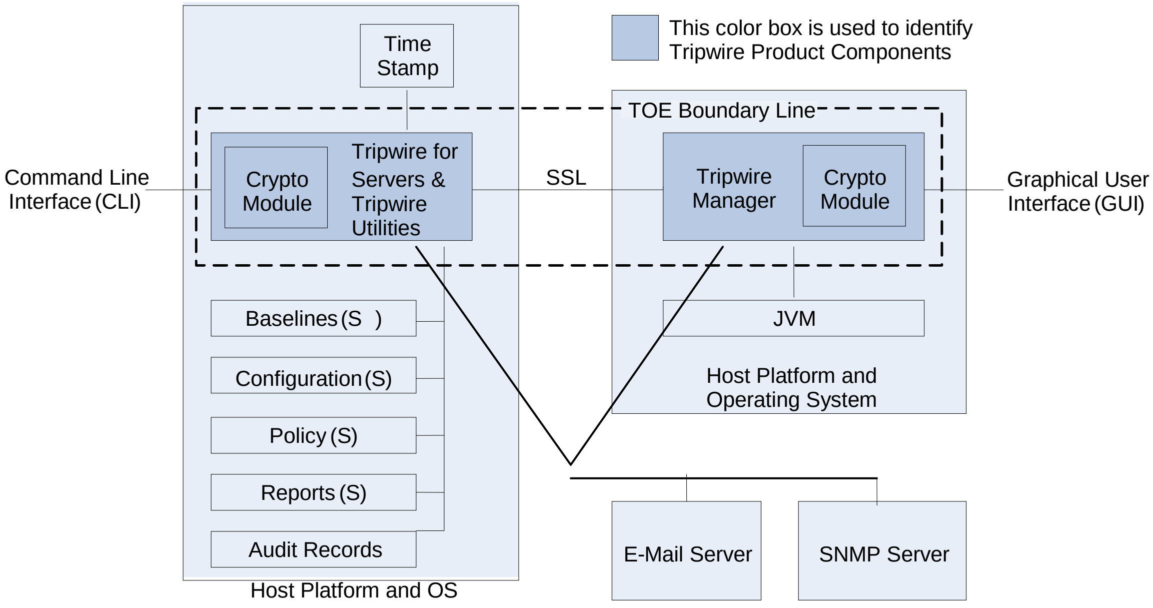
Time Stamp
This color box is used to identify Tripwire Product Components
TOE Boundary Line
Command Line Interface (CLI)
Crypto Module
Tripwire for Servers & Tripwire Utilities
SSL
Tripwire Manager
Crypto Module
Graphical User Interface (GUI)
Baselines (S)
Configuration (S)
Policy (S)
Reports (S)
Audit Records
JVM
Host Platform and Operating System
E-Mail Server
SNMP Server
Host Platform and OS

Figure 1: The TOE and its Environment

6 Documentation

Following is a list of documents supplied by the developer when downloaded from the Tripwire website or shipped with the product.

- Tripwire for Servers 4.6 User Guide, TW1005-12
- Tripwire Manager 4.6 User Guide, TW1004-10
- Tripwire Manager 4.6 Quick Start, TW1052-07
- Tripwire Manager & Tripwire for Servers 4.6 Reference Guide, TW1003-13
- Tripwire for Servers for UNIX Quick Reference Card, TW1007-06
- Tripwire for Servers for Windows Quick Reference Card, TW1008-07
- Tripwire® for Servers Installation Guide 4.6, TW1002-12
- Release notes and readme files:
  - Tripwire for Servers version 4.6.1 Release Notes Addendum December 2008
  - Tripwire for Servers 4.6.1 README December 2008
  - Tripwire Manager 4.6.1 README December 2008
  - Tripwire for Servers version 4.6.1 for Windows December 2008
  - Tripwire for Servers version 4.6.1 for UNIX Operating Systems December 2008
  - Tripwire Manager version 4.6.1 December 2008

The security target used is:

- Tripwire, Inc. Tripwire Manager, Version 4.6.1, with Tripwire for Servers, Version 4.6.1 Security Target, Version 1.0, 1 May, 2009

The following summarizes the evidence used for the evaluation.

Design documentation:

- Tripwire Manager and Tripwire for Servers v4.6 Design Document (HLD, FSP, and RCR)
- Tripwire for Servers 4.6 User Guide, TW1005-12
- Tripwire Manager 46 User Guide, TW1004-10
- Tripwire Manager & Tripwire for Servers 4.6 Reference Guide, TW1003-13
- Tripwire for Servers for UNIX Quick Reference Card, TW1007-06
- Tripwire for Servers for Windows Quick Reference Card, TW1008-07

Guidance documentation:

- Tripwire for Servers 4.6 User Guide, TW1005-12
- Tripwire Manager 4.6 User Guide, TW1004-10
- Tripwire Manager 4.6 Quick Start, TW1052-07
- Tripwire Manager & Tripwire for Servers 4.6 Reference Guide, TW1003-13
- Tripwire for Servers for UNIX Quick Reference Card, TW1007-06
- Tripwire for Servers for Windows Quick Reference Card, TW1008-07
- Tripwire® for Servers Installation Guide 4.6, TW1002-12
- Release notes and readme files:
    - Tripwire for Servers version 4.6.1 Release Notes Addendum December 2008
    - Tripwire for Servers 4.6.1 README December 2008
    - Tripwire Manager 4.6.1 README December 2008
    - Tripwire for Servers version 4.6.1 for Windows December 2008
    - Tripwire for Servers version 4.6.1 for UNIX Operating Systems December 2008
    - Tripwire Manager version 4.6.1 December 2008

Configuration Management and Life-cycle Support:

- Tripwire, Inc. Tripwire Enterprise 5.2, Tripwire for Servers 4.6.1, Tripwire Manager 4.6.1 Configuration Management Plan, TW-ACM1-04
- Tripwire, Inc. Tripwire Enterprise 5.2, Tripwire for Servers 4.6, Tripwire Manager 4.6 Lifecycle, TW-ALC1-03, Version 0.3, September 21, 2007

Delivery and Operation documentation:

- Tripwire Manager and Tripwire for Servers Delivery Procedures Delivery Procedures, TW-TFSADO1-08
- Tripwire Manager 4.6 Quick Start, TW1052-07

- Tripwire® for Servers Installation Guide 4.6, TW1002-12
- Release notes and readme files:
    - Tripwire for Servers version 4.6.1 Release Notes Addendum December 2008
    - Tripwire for Servers 4.6.1 README December 2008
    - Tripwire Manager 4.6.1 README December 2008
    - Tripwire for Servers version 4.6.1 for Windows December 2008
    - Tripwire for Servers version 4.6.1 for UNIX Operating Systems December 2008
    - Tripwire Manager version 4.6.1 December 2008

Test documentation:

- Tripwire, Inc Tripwire Manager and Tripwire for Servers Common Criteria Test Plan
- Test Case Spreadsheet
- Test Procedures and Actual Results

Vulnerability Assessment documentation:

- Tripwire, Inc. Tripwire for Servers 4.6, Tripwire Manager 4.6 Strength of Function Analysis
- Tripwire Manager and Tripwire for Servers version 4.6, Vulnerabilities Assessment
- Guidance documentation (see above)

7 IT Product Testing

The evaluation team applied each EAL 3 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The following tasks were performed by the evaluation team:

The developer test suite was examined and found to provide adequate coverage of the security functions.

A selection of the developer tests were run and the results found to be consistent with the results generated by the developer.

No vulnerabilities in the TOE were found during a search of vulnerability databases.

8 Results of the Evaluation

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

9 Validator Comments/Recommendations

1. The TOE doesn't do individual user identification, only role authorization. However, this is *not* Role-Based Access Control (RBAC), for RBAC identifies individuals to roles. This is a group account, and it makes the TOE unable to satisfy NIST or DOD IA controls regarding accountability.
2. The administrator is a role based account on the TOE, so the administrator password will be shared between the individuals who fill that role. It is important that the password be changed whenever an administrator leaves that role.
3. The ST uses the term "passphrase", but this is misleading as a passphrase is usually multiple words. What this TOE uses is an 8-character password with a complexity that is actually weaker than required by NIST or the DOD.
4. The passphrase is used to construct a key used to encrypt and decrypt critical data. As noted above, it is shared and hence critical that it be changed in conjunction with administrative personnel changes. However, while the passphrase can be changed the process for doing so is onerous and requires leaving target systems unmonitored for a period of time while so doing.
5. Auditing is not enabled by default, and must be specifically enabled in the evaluated configuration. This is a configuration option and not a runtime command and the act of disabling and enabling the audit mechanism is not auditable.
6. Pass-phrase based encryption of *console.dat* is not a method approved by CMVP for FIPS 140-2 cryptographic modules to protect keys.
7. Asymmetric El Gamal keys are used to sign various files stored by the TOE and this is not a FIPS approved algorithm.
8. The TOE makes use of SHA-1 which is going to be obsolete after 2010.
9. The El Gamal implementation used to sign various files stored by the TOE has not been verified through evaluation. There is only developer assurance that the algorithm is implemented correctly.
10. There are no facilities provided for "password frustration" (e.g., lockouts after multiple failures). As such, repeated passphrase guesses can be made without any notion of locking or limiting the account in order to thwart guessing attempts.
11. Cryptographic keys are preconfigured and not checked for correctness By the TOE and as such are only as valid or secure as the hosting environment allows or requires.
12. For the external email server, use of the SMTP protocol is generally insecure and as such users of the TOE should carefully consider whether there is any risk in their deployment.
13. Internationalization aspects of the product were not covered by the evaluation (i.e., the use of multibyte characters)
14. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.
15. The connection between the Tripwire for Servers and Tripwire Manager components is protected with TLSv1 using the RSA-RC4-MD5 ciphersuite. RSA uses 2048 bit keys, and is a good algorithm selection and strength, but RC4 and MD5 are not FIPS

approved algorithms. The validators believe this ciphersuite should be strengthened in upcoming versions of the product.

10 Annexes

Not applicable.

11 Security Target

The security target for this product's evaluation is Tripwire, Inc. Tripwire Manager, Version 4.6.1, with Tripwire for Servers, Version 4.6.1 Security Target, Version 1.0, 1 May, 2009

12 Glossary

There were no definitions used other than those used in the CC or CEM.

Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 2005, version 2.3.

[7] Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R.

[8] Evaluation Technical Report for Tripwire Manager, version 4.6.1 with Tripwire for Servers, version 4.6.1 Part II, version 1.0, 1 May, 2009.

[9] Tripwire, Inc. Tripwire Manager, Version 4.6.1, with Tripwire for Servers, Version 4.6.1 Security Target, Version 1.0, 1 May, 2009.

[10] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.