National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

FireEye xAgent

Report Number: CCEVS-VR-10697-2016

Dated: 07/08/16

Version: 0.1

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers, Senior Validator

Kelly Hood, Validator

Kenneth Stutterheim, Lead Validator

The Aerospace Corporation

Common Criteria Testing Laboratory

W. Dean Freeman, CISSP GCIH

Pascal Patin, CISSP

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 9, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the FireEye Endpoint Agent Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in July 2016. The information in this report is largely derived from the proprietary documents produced by Acumen Security; the Evaluation Technical Report (ETR) and associated detailed test report as summarized in the Common Criteria SWAPP Assurance Activity Report. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for Application Software, version 1.1.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the Protection Profile for Application Software. 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 provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). 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). Based on these findings, 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.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	FireEye Endpoint Agent Version 21
Protection Profile	Protection Profile for Application Software, version 1.1, dated 05 November 2014
Security Target	FireEye Endpoint Agent Security Target, version 1.0
Evaluation Technical Report	VID 10697 Common Criteria SWAPP Assurance Activity Report
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	FireEye, Inc.
Developer	FireEye, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	Jerry Myers, Kelly Hood, Ken Stutterheim

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Overview

The TOE is a software agent that resides on a host platform. The software received policies from an external HX series appliance (validated separately, VID10675). These policies are used to identify potential intrusions on the host platform. The TOE uses these policies to scan the host Operating System to identify indicators of compromise.

3.2 TOE Architecture

3.2.1 Physical Boundaries

The TOE boundary is the application software which runs on the host platform. The software is pushed to the host platform from a FireEye HX series and installs natively as a kernel and user space application. The software runs on Microsoft Operating Systems. The following Operating Systems are included in this evaluation,

- Windows 7 (SP1) x64 running on an Intel Xeon processor
- Windows 7 (SP1) x32 running on an Intel Xeon processor
- Windows Server 2012R2 x64 running on an Intel Xeon processor
- Windows Server 2008R2 (SP1) x64 running on an Intel Xeon processor
- Windows 10 x64 running on an Intel Xeon processor
- Windows 10 x32 running on an Intel Xeon processor

3.2.2 Security Functions provided by the TOE

The TOE provides the security functionality required by the Protection Profile for Application Software.

3.2.2.1 Cryptographic Support

The TOE provides cryptographic support for the following features,

- TLS connectivity with the following entities:
  - HX Series Appliance
- Digital certificate generation

The cryptographic services provided by the TOE are described below.

Cryptographic Method	Use within the TOE
RSA Signature Services	Used in TLS session establishment. Used in secure software update.
SP 800-90 DRBG	Used in TLS session establishment. Used in digital certificate generation.
SHS	Used in secure software update. Used in digital certificate generation.

Cryptographic Method	Use within the TOE
HMAC-SHS	Used to provide TLS traffic integrity verification.
AES	Used to encrypt TLS traffic Secure certificate storage

TOE Provided Cryptography

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below. Each of these algorithms are implemented as part of the OpenSSL cryptographic library, version 1.0.1.

Algorithm	Standard	CAVP Certificate #	Processor
RSA	FIPS PUB 186-4 (Signature generation/verification)	Cert. #1976, 1977	Intel Xeon
SP 800-90 DRBG	SP 800-90	Cert. #1103, 1104	Intel Xeon
SHS	FIPS Pub 180-4	Cert. #3194, 3195	Intel Xeon
HMAC-SHS	FIPS Pub 198-1, FIPS Pub 180-4	Cert. #2517, 2518	Intel Xeon
AES	NIST SP 800-38A	Cert. #3873, 3874	Intel Xeon

CAVP Algorithm Testing References

3.2.2.2 Secure Software Update

The TOE is distributed as a Microsoft .MSI file providing a consistent and reliable versioning. After initial installation, all updates to the xAgent are distributed as .MSI. Each TOE installation and update is signed by FireEye and can only come from the HX Series appliance associated with the TOE.

3.2.2.3 Protection of the TSF

The TOE employs several mechanisms to ensure that it is secure on the host platform. The TOE never allocates memory with both write and execute permission. The TOE is designed to operate in an environment in which the following security techniques are in effect, Data execution prevention, Mandatory address space layout randomization (no memory map to an explicit address), Structured exception handler overwrite protection, Export address table access filtering, Anti-Return Oriented Programming, and SSL/TLS certificate trust pinning. This allows the TOE to operate in an environment in which the Enhanced Mitigation Experience Toolkit is also running. During compilation the TOE is built with several flags enabled that check for engineering flaws. The TOE is built with the /GS flag enabled. This reduces the possibilities of stack-based buffer overflows in the product.

3.2.2.4 Trusted Path/Channels

The TOE receives scanning policies from the associated HX Series appliance over the network which it uses on the host platform. This connection is always secured using TLS.

4 Assumptions, Threats & Clarification of Scope

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

ID	Assumption
A.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

4.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

ID	Threat
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

4.3 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Application Software.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities included in the product were not covered by this evaluation.

5 Documentation

The guidance documentation examined during the course of the evaluation and delivered by the vendor with the TOE is as follows:

- FireEye Endpoint Agent Security Target, Version 1.0, July 2016
- Common Criteria FireEye Endpoint Agent Addendum, Release 21

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when configuring and using the product as evaluated.

6 TOE Evaluated Configuration

6.1 Evaluated Configuration

The TOE boundary is the application software which runs on the host platform. The software is pushed to the host platform from a FireEye HX series and installs natively as a kernel and user space application. The software runs on Microsoft Operating Systems. Certification evaluation has been performed on the following Windows platforms:

- Windows 7 (SP1) x64 running on an Intel Xeon processor
- Windows 7 (SP1) x32 running on an Intel Xeon processor
- Windows Server 2012R2 x64 running on an Intel Xeon processor
- Windows Server 2008R2 (SP1) x64 running on an Intel Xeon processor
- Windows 10 x64 running on an Intel Xeon processor
- Windows 10 x32 running on an Intel Xeon processor

Though the TOE may have the ability to be configured in multiple ways, the evaluated configuration is described in the *Common Criteria FireEye Endpoint Agent Addendum*, Release 21.

6.2 Excluded Functionality

Specific functionality that is outside of the scope of this evaluation include the IDS functionality and the data at rest payloads encrypted within agent encrypted data.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Technical Report, which is not publically available. The Assurance Activity Report, provides an overview of testing and the prescribed assurance activities.

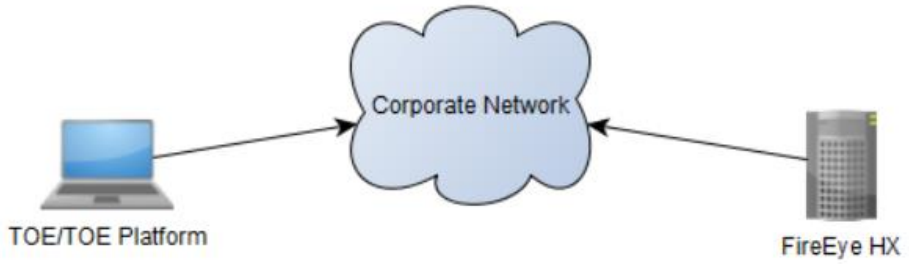
7.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for Application Software. The Independent Testing activities are documented in the *Common Criteria SWAPP Assurance Activity Report,* which is not duplicated here.

Below is a visual representation of the components included in the test bed:



8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the FireEye Endpoint Agent to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the PP.

8.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the FireEye Endpoint Agent that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the Protection Profile for Application Software.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally the evaluator performed the Assurance Activities specified in the Protection Profile for Application Software related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

8.3 Evaluation of Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of

the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the Protection Profile for Application Software related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

8.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the Protection Profile for Application Software and recorded the results in a proprietary Test Report, summarized those in an evaluation sensitive Evaluation Technical Report and provided an synopsis in the publically available Assurance Activities Report.

The validators reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the Protection Profile for Application Software, and that the conclusion reached by the evaluation team was justified.

8.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the Protection Profile for Application Software, and that the conclusion reached by the evaluation team was justified.

8.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the Protection Profile for Application Software, and correctly verified that the product meets the claims in the ST.

9 Validator Comments & Recommendations

The TOE is an enterprise managed agent that runs in the background of an endpoint platform. It is designed such that it requires no end user interaction and is managed at the organizational level. It is intended that the user will have no interaction with the software and will not be alerted of communications with the external HX appliance. The software as evaluated integrates with Microsoft Operating Systems running on Intel Xeon platforms as specified.

Administrators should take note that in the evaluated configuration, the OS host upon which the Agent is installed must have Windows BitLocker enabled. Data at rest payloads are encrypted within agent encrypted data, but are not evaluated.

Testing performed as part of the vulnerability assessment was limited to running an antivirus program, Microsoft Defender, to verify that no malicious files were present in the TOE.

It should also be noted that while this TOE is part of a FireEye IDS solution, the IDS functionality was not tested as a part of this evaluation.

10 Annexes

Not applicable.

11 Security Target

FireEye Endpoint Agent Security Target, Version 1.0, June 2016

12 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 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, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Protection Profile for Application Software, version 1.1
6. FireEye Endpoint Agent Security Target, Version 1.0, July 2016
7. Common Criteria FireEye Endpoint Agent Addendum, Release 21
8. Common Criteria SWAPP Assurance Activity Report, version 1.0
9. Test Plan for FireEye Endpoint Agent, WIN7x32, Version 3.0, June 2016
10. Test Plan for FireEye Endpoint Agent, WIN7x64, Version 2.0, June 2016
11. Test Plan for FireEye Endpoint Agent, WIN10x32, Version 2.0, June 2016
12. Test Plan for FireEye Endpoint Agent, WIN10x64, Version 2.0, June 2016
13. Test Plan for FireEye Endpoint Agent, WIN2008R2, Version 2.0, June 2016
14. Test Plan for FireEye Endpoint Agent, WIN2012R2, Version 1.1, November 17, 2015
15. FireEye X-Agent Security Target Evaluation Technical Report, Version 1.4, July 2016