National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Check Point Endpoint Security Media Encryption

Report Number: CCEVS-VR-VID10231-2010
Dated: 16 July 2010
Version: 1.0

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

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is the Check Point Endpoint Security Media Encryption product. The TOE was evaluated by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed in July 2010. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.3 and the Common Methodology for IT Security Evaluation (CEM), Version 2.3. The evaluation was for Evaluation Assurance Level 4 (EAL4) augmented with ALC_FLR.3 (Parts 2 and 3 conformant). The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The TOE is a workstation security software product that provides centrally managed control of workstation device interfaces. The product can be configured to prevent use of unauthorized devices, and to block introduction of executable code via workstation device ports. A removable media device encryption capability complements device access control, ensuring that only authorized users can access media contents.

This Validation Report presents the evaluation results, their justifications, and the conformance results. The technical information included in this report was largely derived from the Evaluation Technical Report and associated test reports produced by the evaluation team. The Check Point Endpoint Security Media Encryption Security Target, Version 1.0, dated June 23, 2010 identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the Check Point Endpoint Security Media Encryption product by any agency of the US Government and no warranty of the product is either expressed or implied.

Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 Validated Products 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 to which the product is conformant; and
- 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:	Check Point Endpoint Security Media Encryption 4.95 HFA 01 build 238
Protection Profile	None
ST:	Check Point Endpoint Security Media Encryption Security Target, Version 1.0, June 23, 2010
Evaluation Technical Report	Evaluation Technical Report for Check Point Endpoint Security Media Encryption, Part 1 (Non-Proprietary), Version 1.0, 20 May 2010, Part 2 (Proprietary), Version 3.0, 6 July 2010.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

Item	Identifier
Conformance Result	CC Part 2 and Part 3 conformant, EAL 4 augmented with ALC_FLR.3
Sponsor	Check Point Software Technologies Inc.
Developer	Check Point Software Technologies Inc.
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation (SAIC), Columbia, MD

2 Organizational Security Policy

A given instance of the TOE consists of one or more Endpoint Security Media Encryption Server instances using a shared database installation (in the IT environment) and one or more ME client installations associated with that server installation.

The Endpoint Security Media Encryption Server application is installed as a service in the context of the Microsoft Windows 2000 and 2003 Server Edition operating system. TOE Administrators manage the application using the Endpoint Security Media Encryption Server Administration Console, a Microsoft Management Console (MMC) snap-in, installed either locally or remotely to the server. They can configure the policies to be enforced within the associated clients and manage audit data coming back from associated clients. A single SQL or MSDE database server, outside the TOE, is used by all server application instances in order to store client configuration data and audit records. Multiple Administration Consoles instances may be installed and used; however, only a single concurrent instance may be used in the evaluated configuration for updating the database.

The ME client runs in the context of Microsoft Windows 2000 and XP Professional, Windows Vista, and Windows 2000 Server Edition operating systems. When installed according to the available guidance, ME offers a number of security features designed to protect the host operating system as well as data stored on removable media devices and removable media. The protection features, most specifically, revolve around controlling access to removable I/O devices and removable media and encrypting data on removable media devices and removable media to ensure it remains protected even when taken out of the scope of ME control.

3 Assumptions and Clarification of Scope

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be employed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product and defines the threats that the product is designed to counter.

Following are the assumptions identified in the Security Target:

- It is assumed the TOE server component will be located within controlled access facilities, which will prevent unauthorized physical access.
- It is assumed the TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

Following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

- A user may not be held accountable for their actions.
- An authorized administrator may not have tools suitable to allow the effective management of the TOE security functions.
- An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.
- A malicious user may cause the TOE or its configuration data to be inappropriately accessed (viewed, modified or deleted).
- A user may gain unauthorized access (view, modify, delete) to removable I/O devices or data stored within removable media devices.

The TOE is Check Point Endpoint Security Media Encryption is a workstation security software product that provides centrally-managed control of workstation device interfaces. The product can be configured to prevent use of unauthorized devices, and to block introduction of executable code via workstation device ports. A removable media device encryption capability complements device access control, ensuring that only authorized users can access media contents.

The Target of Evaluation includes Endpoint Security Media Encryption Server software used to manage Endpoint Security Media Encryption endpoints. Administrators can publish flexible device access policies and review detailed audit logs of endpoint workstation device access events.

4 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target.

A given instance of the TOE consists of one or more Endpoint Security Media Encryption Server instances using a shared database installation (in the IT environment) and one or more ME client installations associated with that server installation.

The Endpoint Security Media Encryption Server application is installed as a service in the context of the Microsoft Windows 2000 and 2003 Server Edition operating system. TOE Administrators manage the application using the Endpoint Security Media Encryption Server Administration Console, a Microsoft Management Console (MMC) snap-in, installed either locally or remotely to the server. They can configure the policies to be enforced within the associated clients and manage audit data coming back from associated

clients. A single SQL or MSDE database server, outside the TOE, is used by all server application instances in order to store client configuration data and audit records. Multiple Administration Consoles instances may be installed and used; however, only a single concurrent instance may be used in the evaluated configuration for updating the database.

When the ME clients are installed, they are configured with the IP addresses of the associated servers. They will use these addresses to contact a server, where a unique identifier will be created for identification of that client, in order to obtain the policy configuration it will enforce. Subsequently, the client will receive policy updates from the server at configured intervals or in response to a request for a policy update. In addition, the client will forward any audit records it has generated either at a configured interval or immediately depending on the nature of the event.

The ME clients consist of drivers installed as filters within the operating system kernel, a service to facilitate communication with the server, and some other applications to instantiate a limited set of pop-up and tray icon functions (if so configured). Once installed, the client is mostly transparent to the user. There is a tray icon where they can review the status of the product and perceive that it is operating and, depending on the specific configuration, the user may see pop-ups when specific security-relevant events occur (e.g., disallowed attempt to use a removable media device). Depending on policy settings received from the server, the user may be able to perform limited management activities, such as authorizing or importing (encrypting) removable media devices, and setting removable device off-line access passwords.

The ME client drivers serve to:

- allow the client to become aware of new removable I/O devices or removable media introduced to the operating system and to control (i.e., by blocking disallowed access attempts within the kernel) the ability to use those devices in accordance with its configured policies;
- allow the client to sign removable media devices each time its contents are changed and to verify the signature when removable media is introduced, and to take configured actions when the signature is not correct (e.g., invoke a third-party scanning program, allow offending content to be deleted, disallow access altogether);
- allow the client to intercept and encrypt and decrypt data between user mode applications and removable media devices or removable media;
- allow the client to intercept attempts to create or modify specific types of files in order to enforce (i.e., by blocking disallowed file operations) its configured PSG policies; and
- allow the client to monitor file and registry access attempts so that it can protect its own binary and data files and keys to ensure its own functions cannot be disabled or otherwise tampered with.

When the ME client observes security-relevant events, such as an attempted violation of its configured polices, it can create an audit record of that event. The audit records are stored in a database implemented within the client and forwarded to the associated Endpoint

Security Media Encryption Server at a configured interval. The exception is that specific events can be configured to be reported immediately and when those occur the client will forward that audit record to the server as soon as possible regardless of the configured reporting interval.

As indicated above, the ME client enforces the policy configured on the associated server and delivered to the client. The client offers no interfaces to manage its own policies and controls access to its configuration data so that even an administrator on the client operating system has no ready means (e.g., to modify the configuration data directly) to change the configuration.

Communication between the Endpoint Security Media Encryption Server and the ME clients as well as communication with the Administration Console is based on the hosting Microsoft Windows operating system's Security Service Provider Interface (SSPI using the NTLM SSP) for providing user identification and authentication and for encryption of data in transit. The Endpoint Security Media Encryption Server uses operating system user account and group assignments for assigning users to management roles, for selecting the policy profile to be applied by the client, and for enforcing access control to encrypted media. User group assignments may also be synchronized with a Novell NDS directory.

5 Documentation

Following is a list of the non-proprietary evaluation evidence that is available to the end-user.

5.1 Guidance documentation

Document	**Version**	**Date**
Check Point Endpoint Security Media Encryption Administration Guide	Version R71	January 22, 2009
Endpoint Security Media Encryption CC Evaluated Configuration Administrator's Guide	Version R71	June 23, 2010
Endpoint Security Media Encryption CC Evaluated Configuration User's Guide	Version R71	February 1, 2010
Check Point Endpoint Security Media Encryption Installation Guide	Version R71	January 22, 2009
Check Point Endpoint Security Client Installation Guide	Version R71	December 3, 2008

5.2 Security Target

Document	**Version**	**Date**
Check Point Endpoint Security Media Encryption Security Target	Version 1.0	June 23, 2010

6 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

6.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function, more specifically to the security functional requirements tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security audit, Cryptographic support, User Data Protection, Identification and authentication, Security management, and Protection of the TSF. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

6.2 Evaluation Team Independent Testing

The evaluation team exercised a subset of the vendor's manual test suite in the following test configurations, a General TC used for the bulk of the test procedures, an Extended TC used for testing special configurations of the product, e.g. the connection to the Novell Directory, and an Anti Virus TC used for testing the integration with supported anti-v
5) that do not explicitly specify a different TC should be run on the General TC.

In addition to exercising the vendor's tests, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All team tests were run as manual tests.

The vendor provided a Windows 2003 machine, the Windows XP machines, printer, scanner, USBs, and external CD/DVD. The CCTL provided the Windows Vista machine, Windows XP machine, and the necessary network peripheral devices, such as hubs and cabling.

The following hardware and software is necessary to create the test configuration:

The General TC assumes the following test platforms are configured with the following characteristics, all connected to a network switch or hub:

- **VMWare Workstation version 6.5 -** running the following machine images:
  - **DC** - Windows 2003 Server
    - Windows Domain Controller and Active Directory
    - SMTP server
  - **MESRV** – Windows 2000 Server or Windows 2003 Server[1]

[1] The ME server operating system may be any one of the supported Windows Server operating system versions. This test plan does not require retesting on each individual version, as the ME server subsystem is implemented using high-level services that do not rely on nor leverage any version-specific interfaces or

- Member of DC Windows domain
- ME server
- SQL Server database

- **MEPC** – Windows XP Professional installed on laptop
  - Member of DC Windows domain
  - ME client
  - USB-connected scanner device
  - Parallel port-connected printer
  - Floppy disk drive and CD-ROM R/W drive
  - Internally-connected modem
- **NONMEPC** – Windows XP Professional installed on a laptop

The Extended TC uses the same computer hardware and switch or hub as the General TC. In addition, the following test platform is connected to the switch or hub:

- **MEPC_V** – Windows Vista (32 bit)
  - Member of DC Windows domain
  - ME client in non-integrated mode
  - DVD R/W drive
  - ME server
  - SQL Server database
- **MEPC_N** – Windows XP Professional
  - ME client

The Anti Virus TC is used for testing the integration with supported anti-virus products. It uses the same computer hardware and switch or hub as the General TC. The following anti-virus products are included in the Anti Virus TC: Symantec AntiVirus Corporate Edition, McAfee VirusScan 8.5, Trend micro 5, AVG 7, and Sophos 5.

In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

6.3 Vulnerability Testing

The evaluators developed vulnerability tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

---

functionality. Note that testing is performed on each supported ME client operating system version, because the ME client drivers do contain operating system version-specific code (e.g. for CD/DVD burning).

7 Evaluated Configuration

The evaluated configuration consists of a given instance of the TOE consists of one or more Endpoint Security Media Encryption Server instances using a shared database installation (in the IT environment) and one or more ME client installations associated with that server installation.

The Endpoint Security Media Encryption Server application is installed as a service in the context of the Microsoft Windows 2000 and 2003 Server Edition operating system.

The ME clients consist of drivers installed as filters within the operating system kernel, a service to facilitate communication with the server, and some other applications to instantiate a limited set of pop-up and tray icon functions (if so configured). Once installed, the client is mostly transparent to the user.

For specific configuration settings required in the evaluated configuration see Endpoint Security Media Encryption CC Evaluated Configuration Administrator's Guide.

8 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM. A Pass, Fail, or Inconclusive verdict was assigned to each work unit of assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing notes, comments, or vendor actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The criteria and evaluation methodology against which the Endpoint Security Media Encryption TOE was judged are described in the CC and CEM, Version 2.3, dated August 2005; and all applicable International Interpretations in effect on July 2007. The SAIC CCTL determined that the evaluation assurance level (EAL) for the Check Point Endpoint Security Media Encryption TOE is EAL 4 and that the TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target. The results of the evaluation and the rationale supporting each CEM work unit verdict are recorded in the Check Point Endpoint Security Media Encryption Evaluation Technical Report which is considered proprietary.

9 Validator Comments/Recommendations

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

10 Security Target

The Check Point Endpoint Security Media Encryption Security Target, Version 1.0, June 23, 2010 identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4 augmented with ALC_FLR.3.

11 Glossary

The following definitions are used throughout this document:

CC	Common Criteria
GUI	Graphical User Interface
HTTP	Hyper-text Transfer Protocol
HTTPS	Secure HTTP
ID	Identity / Identification
IE	Internet Explorer
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PC	Personal Computer
PD	Precedent Decision
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation

12 Bibliography

Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

Evaluation Technical Report For Check Point Endpoint Security Media Encryption Part 1 (Non-Point Proprietary) Version 1.0, 20 May 2010.

Evaluation Technical Report For Check Point Endpoint Security Media Encryption Part 2 (SAIC and Check Point Proprietary) Version 3.0, 6 July 2010 and Supplemental Team Test Report, Version 1.0, 20 May 2010.

Check Point Endpoint Security Media Encryption Security Target, Version 1.0, June 23, 2010.