National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

McAfee

Foundstone Enterprise Vulnerability Management Solution Version 5.0.4

Report Number: CCEVS-VR-VID10241-2007

Dated: 7 December 2007

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)

Aerospace Corporation

Columbia, Maryland

Dr. Jerome F. Myers (Senior Validator)

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

COACT CAFÉ Laboratory

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated. Prospective users should read the Validator Comments in Section 10 carefully.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the McAfee® Enterprise Vulnerability Management Solution Version 5.0.4, the target of evaluation (TOE), conducted by the CAFÉ Laboratory of COACT Incorporated, the Common Criteria Testing Laboratory (CCTL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation by COACT was performed in accordance with the United States evaluation scheme and was completed on September 13th, 2007. The information in this report is largely derived from the ST, Evaluation Technical Report (ETR) and the functional testing report. The ST was written by McAfee® Incorporated. The evaluation was performed to conform with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005 Evaluation Assurance Level 2 (EAL 2) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.3, August 2005.

The TOE is a software product that provides a Vulnerability Management System that scans specified targets for IP-level vulnerabilities based on the ports and protocols used by the target systems. It provides a management interface to configure the system and generate reports regarding the results of the scans.

Foundstone Enterprise consists of three main components:

A) The Foundstone Enterprise Manager uses Microsoft Internet Information Services (IIS) to provide authorized users with access to Foundstone Enterprise through their Web browsers. It allows them to manage and run Foundstone Enterprise from anywhere on the network. Access is protected by user identification and authentication.

B) One or more FoundScan Engines scan the network environment. Depending on the logistics and size of a network, more than one FoundScan Engine may be needed to ensure efficient operation of the scanners. The one required FoundScan Engine is referred to as the primary engine. All others (if present) are referred to as secondary engines.

C) The Foundstone Database is the data repository for the Foundstone system. It uses Microsoft SQL Server to store everything from scan settings and results to user accounts and FoundScan Engine settings. It contains all of the information needed to track organizations and workgroups, manage users and groups, run scans, and

generate reports. A stipulation of the evaluated configuration is that the system that hosts the database must not service any other databases.

All traffic between the components is encrypted for secure communication.

Microsoft IIS and SQL Server 2000 are considered to be part of the Information Technology Environment and were not evaluated as part of the product.

Foundstone 5.0.4 supports the Microsoft Internet Explorer 6.0 and higher Web browser, running on Windows 2000 SP2 and higher, Windows 2003 Server, or Windows XP. Latest service packs should be applied to both your browser and operating system. Foundstone 5.0.4 requires the Java Runtime Environment version Java Runtime Environment 1.5.0_06. **NOTE:** If the Runtime Environment is not found on the user's system when it is needed, the user's Web browser will silently install it.

1.1. Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that no international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation. The TOE is also compliant with all International interpretations with effective dates on or before January 26, 2007.

The Evaluation Team determined that the following NIAP interpretations applied at the time of the start of the evaluation:

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3

I-0426 – Content of PP Claims Rationale

I-0427 – Identification of Standards

2. 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 conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	McAfee Foundstone Enterprise Vulnerability Management Solution Version 5.0.4.
Protection Profile	None
Security Target	*McAfee Foundstone Enterprise Vulnerability Management Solution Version 5.0.4 Security Target*, Version 1.11, dated October 25, 2007.
Dates of evaluation	November 2006 through September 2007
Evaluation Technical Report	*Evaluation Technical Report for the McAfee Foundstone Enterprise Vulnerability Management Solution Version 5.0.4*. Document No. F2-0907-001, Dated 30 November 2007.
Conformance Result	Part 2 and Part 3 conformant, EAL 2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on January 26, 2007
Common Evaluation Methodology (CEM) version	CEM version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on January 26, 2007
Sponsor	McAfee Inc., 3965 Freedom Circle, Santa Clara, CA 95054
Developer	McAfee Inc., 3965 Freedom Circle, Santa Clara, CA 95054
Evaluators	Bob Roland, Greg Beaver and Chrisa Lanzisera of COACT Incorporated
Validation Team	Dr. Jerome Myers and Mike Allen of The Aerospace Corporation

3. SECURITY POLICY

The McAfee Foundstone Enterprise Vulnerability Management Solution Version 5.0.4 consists of three main components:

A) The Foundstone Enterprise Manager uses Microsoft Internet Information Services (IIS) to provide authorized users with access to Foundstone Enterprise through their Web browsers. It allows them to manage and run Foundstone Enterprise from anywhere on the network. Access is protected by user identification and authentication.

B) One or more FoundScan Engines scan the network environment. Depending on the logistics and size of the network, more than one FoundScan Engine may be needed to scan the network. The one required FoundScan Engine is referred to as the primary engine. All others (if present) are referred to as secondary engines.

C) The Foundstone Database is the data repository for the Foundstone system. It uses Microsoft SQL Server to store everything from scan settings and results to user accounts and FoundScan Engine settings. It contains all of the information needed to track organizations and workgroups, manage users and groups, run scans, and generate reports. **NOTE:** In order to operate the Foundstone product in the evaluated configuration, the Foundstone Database must be used on a dedicated system that services no other databases.

All traffic between the components is encrypted for secure communication.

The security functions provided by the TOE and are described in the following sections.

3.1.1. Scanning

The TOE scans designated systems to detect known IP-level vulnerabilities on those systems based on the ports and protocols used by the scanned systems. Results of the scans are stored in the database (the DBMS is in the IT Environment), and reports based upon completed scans may be retrieved via the GUI interface of the Foundstone Enterprise manager.

3.1.2. Identification and Authentication (I&A)

The TOE requires users to identify and authenticate themselves before accessing the TOE software or before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that defines the functionality the user is allowed to perform.

When interacting with the TOE via the Foundstone Enterprise Manager GUI, I&A is performed by the TOE. On all three components, I&A for local login to the operating system (i.e., via the local console) is performed by Windows (IT Environment).

3.1.3. Self Protection

The TOE provides for self protection and non-bypassability of functions within the TOE's scope of control (TSC). The TOE controls actions carried out by an administrator by controlling a session and the actions carried out during a session. When multiple administrators are connected simultaneously, the roles (and therefore permissions) are tracked individually to ensure proper access restrictions are applied to each session. By maintaining and controlling each user session a user has with the TOE, the TOE ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE which prevents an inadvertent interference or tampering with the TOE from within the TSC.

Since the TOE consists of a set of applications, the TOE cannot provide complete self-protection for itself. The TOE depends on the operating systems and hardware (IT Environment) to protect the TOE from interference or bypass from users or processes outside the TSC. The IT Environment also provides the SSL functionality used to protect communications between the TOE components.

3.1.4. Management

The TOE's Management Security Function provides administrator support functionality that enables a human user to configure and manage TOE components.

Management of the TOE is performed via the Foundstone Enterprise Manager. All user types use the Foundstone Enterprise Manager.

The TOE provides the following management functions:

A) User management,
B) Root organization management,
C) Workgroup management,
D) FoundScan Engine management,
E) Asset management,
F) Scan management,
G) Report management

3.1.5. Audit

The TOE's Audit Security Function provides auditing of management actions performed by administrators. All audit records include the date and time of the event, type of event, and subject identity performing the action (the user identifier supplied by the user and/or IP address of the browser session associated with the event). The type of event implicitly states whether or not the action succeeded (i.e., there are separate event types for successful and unsuccessful I&A attempts).

Audit records are stored in the Foundstone Database. Administrators are advised to configure the database to expand to the limits of the file system. In the unlikely event storage space exhaustion does occur, the TOE discards the most recent records.

4. ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1. Physical Security Assumptions

A key environmental assumption is physical security, for it is assumed appropriate physical security protection will be applied to the TOE hardware and software commensurate with the value of the IT assets. Specifically, the TOE is assumed to be located in a secure location providing physical protection and limited access to administrators only.

4.2. Personnel Security Assumptions

It is assumed that all authorized administrators are properly trained, not careless, not willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.

4.3. Operational Security Assumptions

It is assumed that the McAfee® Foundstone system is dedicated to its primary function and is not intended to provide any general purpose computing or storage capabilities. In addition, the database subsystem is dedicated to providing database management to the Foundstone product and does not provide any other support to another database user.

4.4. Threats Countered and Not Countered

The TOE and Operating IT Environment are designed to fully or partially counter the following threats:

T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

4.5. Organizational Security Policies

There are no applicable organizational security policies

4.6. Clarification of Scope

The following functionality of Foundstone Enterprise is not included in the evaluation and should not be used by customers desiring the evaluated configuration:

- The optional Remediation Module.
- The optional Threat Correlation Module.
- The optional Notification Module.
- The Foundstone Configuration Manager/Foundstone Update (software updates).
- Integration with a third-party Single-Sign-On server.
- Management via FoundScan Console. NOTE: As part of the TOE installation process, all ability to manage users and reports via FoundScan Console must be disabled. The FoundScan Console is used for initial configuration of the local FoundScan Engine only.

5. ARCHITECTURAL INFORMATION

Foundstone Enterprise is evaluated in a Distributed Server Architecture. This architecture is appropriate for complex organizations where large disparate networks in multiple geographical regions may require multiple FoundScan Engines. The scan engines generate all scanning traffic on their local network segments. The engines send the resulting scan data back over the WAN to the Foundstone Database.

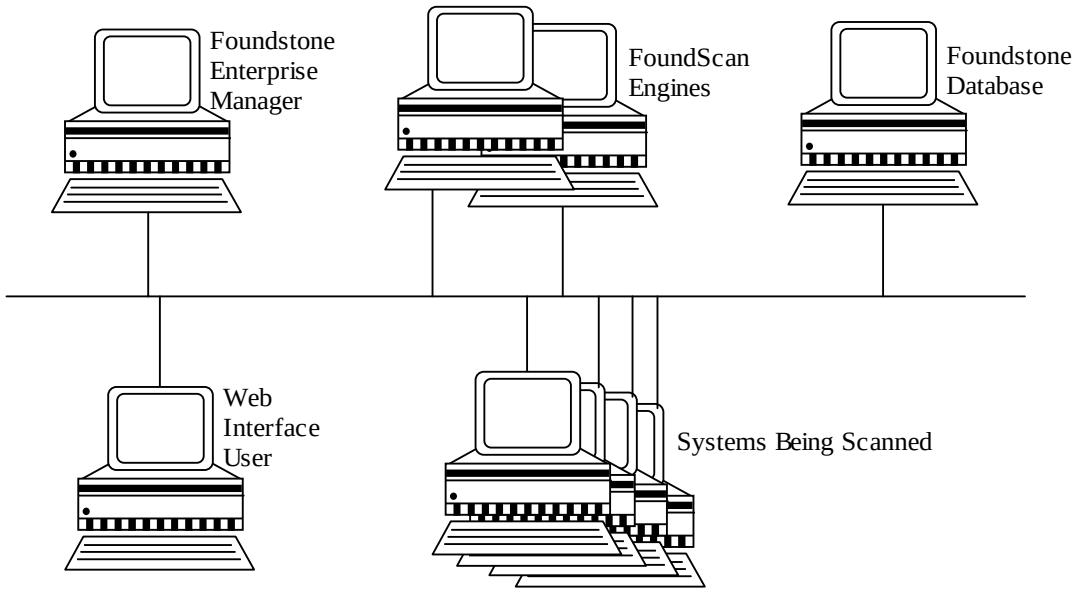
In this architecture the following components exist:

A) One instance of Foundstone Enterprise Manager on a dedicated platform.
B) One instance of FoundScan Engine (primary engine) on a dedicated platform.
C) Zero or more instances of FoundScan Engine (secondary engines) on additional dedicated platforms.
D) One instance of the Foundstone Database hosted on a separate dedicated platform (together with the DBMS).

The evaluated configuration is illustrated in the following figure.

5.1. Evaluated Configuration

Figure 1 - Evaluated Configuration



The platform on which the Foundstone Enterprise Manager software is installed must be dedicated to functioning as the Foundstone Enterprise Manager. The TOE requires the following hardware and software configuration on this platform:

Table 2: Foundstone Enterprise Manager Component Requirements

Component Minimum Requirements	
Processor	Dual Xeon 2Ghz
Memory	2 GB RAM
Disk Space	80GB Partition
Operating System	Windows 2000 Server or Windows Server 2003 Current service pack: Windows 2000 - SP4 (minimum) Windows 2003 - SP1 (minimum) Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023
Additional Software	IIS 5.0 if using Win 2000 Server IIS 6.0 if using Win 2003 Server Current IIS security patches MDAC 2.7 SP1
Network Card	Dual 10/100/1000 Ethernet
Disk Partition Formats	NTFS
Required Services	n/a

5.2. FoundScan Engine (Primary or Secondary) Configuration

The platform on which the FoundScan Engine software is installed must be dedicated to functioning as a FoundScan Engine (Primary or Secondary). The TOE requires the hardware and software configuration in Table 3 on the FoundScan Engine. An Administrator account must be defined on the platform for use by the TOE.

5.3. FoundScan Database Configuration

The platform on which the Foundstone Database is installed must be dedicated to functioning as the database server for the TOE. The DBMS is installed on this same platform and no other databases may be used on this system. The TOE requires the following hardware and software configuration on this platform.

Table 3: FoundScan Engine (Primary or Secondary) Component Requirements

Component Minimum Requirements	
Processor	Dual Xeon 2Ghz
Memory	2 GB RAM
Disk Space	80GB Partition
Operating System	Windows 2000 Server or Windows Server 2003 Current service pack: Windows 2000 - SP4 (minimum) Windows 2003 - SP1 (minimum) Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023
Additional Software	MDAC 2.7 SP1 SQL Client Tools (for Microsoft SQL Server 2000) JRE Java Runtime Environment 1.5.0_06
Network Card	Dual 10/100/1000 Ethernet
Virtual Memory	2.0 GB
Disk Partition Formats	NTFS
Required Services	NetBIOS over TCP/IP Print Spooler

Table 4: Foundstone Database Component Requirements

Component Minimum Requirements	
Processor	Dual Xeon 2Ghz
Memory	2 GB RAM
Disk Space	80GB Partition
Operating System	Windows 2000 Server or Windows Server 2003 Current service pack: Windows 2000 - SP4 (minimum) Windows 2003 - SP1 (minimum) Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023
Additional Software	Microsoft SQL Server 2000 (SP4 and all hotfixes/patches)
Network Card	Dual 10/100/1000 Ethernet
Virtual Memory	2.0 GB
Disk Partition Formats	NTFS
SQL Server Memory Settings	900MB
Required Services	n/a

5.4. Supported Web Browsers

Authorized users can access the Foundstone system through their Web browser software from anywhere on the network, depending on your network settings.

Foundstone 5.0.4 supports Microsoft Internet Explorer 6.0 and higher, running on Windows 2000 SP2 and higher, Windows 2003 Server, or Windows XP. Latest service packs should be applied to both the browser and operating system. Foundstone 5.0.4 requires the Java Runtime Environment version Java Runtime Environment 1.5.0_06. If this is not found on the user's system when it is needed, the user's Web browser silently installs it.

6. DOCUMENTATION

This section details the documentation that is delivered to the customer or was used as evidence for the evaluation of the McAfee® Foundstone Product. These documents are available as part of the download of the product by users with appropriate credentials. Note that not all of the documents were used in the evaluation. Those documents marked with an * were not part of the evaluation and have not been examined or evaluated as to their accuracy.

1. ERM Admin Quickstart Guide.PDF*
2. ERM CSV Reporting User Guide.PDF*
3. ERM FS 1000 Addendum.PDF*
4. ERM Install Guide.PDF*
5. ERM User's Guide.PDF*
6. Foundstone 5.0 Configuration Guide.PDF*
7. Foundstone 5.0 Configuration Manager.PDF
8. Foundstone 5.0 Console Admin Guide.PDF
9. Foundstone 5.0 Database Maintenance Guide.PDF*
10. Foundstone 5.0 Database Utility Guide.PDF*
11. Foundstone 5.0 EM Global Admin Guide.PDF
12. Foundstone 5.0 EM Org Admin Guide.PDF
13. Foundstone 5.0 EM Rem Admin Guide.PDF
14. Foundstone 5.0 EM User Guide.PDF
15. Foundstone 5.0 Installation Guide.PDF
16. Foundstone 5.0 Performance Tuning Guide.PDF*
17. Foundstone 5.0 Release Notes.PDF*
18. Foundstone 5.0 System Requirements.PDF*
19. Foundstone Licenses.PDF*
20. Read Me First.PDF*

7. IT PRODUCT TESTING

This section describes the testing efforts of the Developer and the evaluation team.

7.1. Developer testing

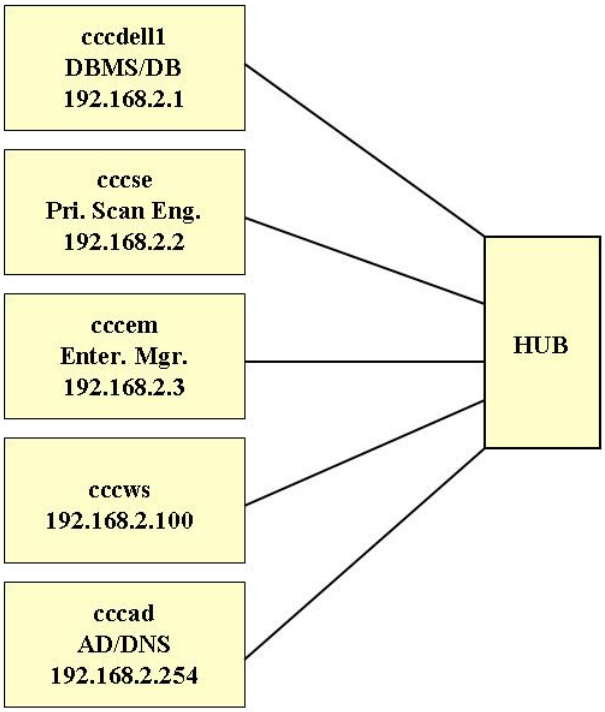
Since the Evaluation team repeated all of the security testing accomplished by the developer, the test descriptions presented below under the Evaluation Team testing provide the documentation of the developer's effort.

The Developer and evaluation team tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. Each test case was identified by a number that correlates to the expected test results in the TOE Test Plan.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 2. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

The following diagrams depict the test environment that was used by the Developers and the Evaluators. The Evaluators assessed that the test environment used by the Developers was appropriate and mirrored the test configuration during Independent testing.

Figure 2 - Test Configuration/Setup



An overview of the purpose of each of these systems is provided in the following table.

Table 5: Test Configuration Overview

System	Purpose
cccdell1	This system provides the Foundstone Database functionality for the testing.
cccse	This system provides the FoundScan Engine functionality for the testing. Only one scan engine is used in the testing.
cccem	This system provides the Foundstone Enterprise Manager functionality for the testing. This system is also scanned for vulnerabilities.
cccws	This system provides a web browser for access to the Foundstone Enterprise Manager. This system is also scanned for vulnerabilities.
cccad	This system provides the Active Directory (AD) and Domain Name System (DNS) infrastructure for the testing.

Specific configuration details for each of the systems are provided in the tables below.

Table 6: cccdell1 Details

System	Installed Components
Installed software	Microsoft Windows 2000 Server SP4 Microsoft Installer (MSI) Version 3.1 Microsoft Data Access Components (MDAC) Vresion 2.8 Microsoft SQL Server 2000 SP4 Microsoft Internet Explorer 6.0 SP1 Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05) JScript update provided in Microsoft Security Bulletin MS06-023 Foundstone 5.0.4 Database Foundstone 5.0.4 Configuration Manager Adobe Reader Version 6.0 WinZip Version 11.1 Opera Version 9.21 FireFox Version 2.0.04 WireShark Version 0.99.4 Snag It Version 8.00
Configuration	Static IP address 192.168.2.1/24 DNS Server 192.168.2.254 FQDN cccdell1.domain2.consulting-cc.com

Table 7: cccse Details

System	Installed Components
Installed software	Microsoft Windows 2000 Server SP4 Microsoft Installer (MSI) Version 3.1 Microsoft Data Access Components (MDAC) Vresion 2.8 Microsoft SQL Server 2000 Client Tools SP4 Microsoft Internet Explorer 6.0 SP1 Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05) JScript update provided in Microsoft Security Bulletin MS06-023 Foundstone 5.0.4 FoundScan Console FoundScan Console Patch 5.0.4 Foundstone Configuration Agent Patch 5.0.2 Adobe Reader Version 8.1 WinZip Version 11.1 FireFox Version 2.0.04 Open Office Version 2.1 Opera Version 9.21 SnagIt Version 8 Nessus Version 3

System	Installed Components
	WireShark Version 0.99.4
Configuration	Static IP address 192.168.2.2/24 DNS Server 192.168.2.254 FQDN cccse.domain2.consulting-cc.com

Table 8: cccem Details

System	Installed Components
Installed software	Microsoft Windows 2000 Server SP4 Microsoft Installer (MSI) Version 3.1 Microsoft Data Access Components (MDAC) Vresion 2.8 Microsoft Internet Information Services Web Server (IIS) IIS Lockdown Tool Microsoft Internet Explorer 6.0 SP1 Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05) JScript update provided in Microsoft Security Bulletin MS06-023 Foundstone 5.0.4 Foundstone Enterprise Manager Adobe Reader Version 6.0 WinZip Version 11.1 FireFox Version 2.0.04 WinCap Version 3.1 SnagIt Version 8.00
Configuration	Static IP address 192.168.2.3/24 DNS Server 192.168.2.254 FQDN cccem.domain2.consulting-cc.com

Table 9: cccws Details

System	Installed Components
Installed software	Microsoft Windows XP Professional SP2 and all patches Microsoft Internet Explorer 6.0 SP2 and all security patches Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05)
Configuration	Static IP address 192.168.2.100/24 DNS Server 192.168.2.254 FQDN cccws.domain2.consulting-cc.com

Table 10: cccad Details

System	Installed Components
Installed software	Microsoft Windows 2000 Server SP4
Configuration	Static IP address 192.168.2.254/24 FQDN cccad.domain2.consulting-cc.com Primary Domain Controller for domain2.consulting-cc.com DNS Server for domain2.consulting-cc.com with records for all systems identified in the test configuration JRE 1.4.2_07 MS Internet Explorer 6 SP1 Open Office Version 2.1 SnagIt Version 8 Wireshark 0.99.4

7.2. Functional Test Results

The repeated developer test suite includes all of the five developer functional tests. Additionally, each of the Security Functions and developer tested TSFIs are included in the CCTL test suite. The results are found in the Foundstone Functional Test Report, Document No. F2-0907-002, dated November 30, 2007.

7.3. Evaluator Independent Testing

The tests chosen for independent testing allow the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests is to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allow for a finer level of granularity of testing compared to the developer's testing, or provide additional testing of functions that were not exhaustively tested by the developer. The tests allow specific functions and functionality to be tested. The tests reflect knowledge of the TOE gained from performing other work units in the evaluation. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests.

7.4. Evaluator Penetration Tests

The evaluators examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. After consulting the sources identified by the developer used during the initial vulnerability analysis, the evaluator consulted other vulnerability relevant sources of information to verify that the developer considered all available information when developing the non-exploitation rationale. These additional sources include:

Table 11: Internet Web Site Vulnerability Searches

Site	Vulnerability ID Prefix	Keywords Used for the Searches
http://www.secunia.com	SA	McAfee, Foundstone, FScan, Java Runtime, JRE
http://cve.mitre.org	CVE	McAfee, Foundstone, FScan, Java Runtime, JRE
http://www.osvdb.org	OSVDB	Vendor; Foundstone; Vendor: McAfee, Product: Foundstone; Vendor: Sun, Product: Java; Vendor: Sun, Product: JRE
http://www.kb.cert.org/vuls/	VU	McAfee, Foundstone, FScan, Java Runtime, JRE
http://www.securityfocus.com	Bugtraq	McAfee, Foundstone, FScan, Java Runtime, JRE
http://www.us-cert.gov/	SA, TA	

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluator made an assessment of the rationales provided by the developer indicting that the vulnerability is non-exploitable in the intended environment of the TOE.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerability.

The evaluator determined that the rationales provided by the developer indicate that the vulnerabilities identified are non-exploitable in the intended environment of the TOE.

7.5. Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

8. EVALUATED CONFIGURATION

The evaluated configuration of the McAfee® Foundstone Product, as defined in the Security Target, consists of the components as described in the testing section. Please refer to Figure 2 and Tables 5 through 10 for the TOE's hardware and software components.

The McAfee® Foundstone Enterprise Vulnerability Management Solution Version 5.0.4 must be configured in accordance with the following additional User Guidance Document available from the McAfee web site:

- McAfee® Corporation's Foundstone Enterprise Vulnerability Management Solution Version 5.0.4 Installation Supplement, Version 1.6, October 25, 2007

9. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

COACT CAFÉ Laboratory has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on September 13, 2007. A final Validation Oversight Review (VOR) was held on October 25, 2007 and final changes to the ST, ETR and VR were completed on November 6, 2007.

10. VALIDATOR COMMENTS

The validation team's observations support the evaluation team's conclusion that the McAfee McAfee® Foundstone Enterprise Vulnerability Management Solution Version 5.0.4 meets the claims stated in the Security Target. The validation team adds the following caveats to the use of the product and the evaluated configuration.

To be used in the evaluated configuration the users of the TOE must **not** make use of the following options and features:

A) The optional Remediation Module.
B) The optional Threat Correlation Module.
C) The Foundstone Configuration Manager/Foundstone Update (software updates).
D) Integration with a third-party Single-Sign-On server.
E) Management via FoundScan Console. **Note:** As part of the TOE installation process, all ability to manage users and reports via FoundScan Console must be disabled. FoundScan Console is only used for initial configuration of the local FoundScan Engine.

In addition, it must be emphasized that the Foundstone Database system must operate on a dedicated machine with no other databases present.

NOTE: It is important for users of the evaluated configuration to obtain the following supplement to the Foundstone User's Guide to ensure proper configuration of the product:

- McAfee® Corporation's Foundstone Enterprise Vulnerability Management Solution Version 5.0.4 Installation Supplement, Version 1.6, October 25, 2007

This document is available to authorized Foundstone users from the McAfee web site.

11. ANNEXES

None

12. SECURITY TARGET

McAfee® Foundstone Enterprise Vulnerability Management Solution Version 5.0.4 Security Target, Version 1.11 dated October 25, 2007

13. GLOSSARY

- **Administrator:** Role applied to user with full access to all aspects of the McAfee® Foundstone Enterprise Vulnerability Management Solution Version 5.0.4.

- **Authentication:** Verification of the identity of a user.

- **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.

- **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.

- **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.

- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.

- **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.

- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

- **Acronym List:**

CC ……Common Criteria

EAL2 ……Evaluation Assurance Level 2

IT ……..Information Technology

NIAP ……..…..National Information Assurance Partnership

PP ……Protection Profile

SF ……Security Function

SFP ……..Security Function Policy

SOF ……Strength of Function

ST …… ….Security Target

TOE ……Target of Evaluation

TSC ……TSF Scope of Control

TSF ……..TOE Security Functions

TSFI ……...……TSF Interface

TSP ……TOE Security Policy

14. BIBLIOGRAPHY

1.) *Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model*, Version 2.3, dated August 2005, CCMB-2005-08-001

2.) *Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements*, Version 2.3, dated August 2005, CCMB-2005-08-002

3.) *Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements*, Version 2.3, dated August 2005, CCMB-2005-08-003

4.) *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, Version 2.3, dated August 2005, CCMB-2005-08-004

5.) *Guide for the Production of PPs and STs*, Version 0.9, dated January 2000

6.) *McAfee® Corporation's Foundstone Enterprise Vulnerability Management Solution Version 5.0.4 Security Target*, Version 1.11, October 25, 2007

7.) CAFÉ Laboratory of COACT Incorporated, *Evaluation Technical Report for McAfee® Foundstone Enterprise Vulnerability Management Solution*, Version 5.0.4, September 13, 2007, Document No. E2-0907-001