National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

HP Network Node Management Advanced Edition Software V7.51 with patch PHSS_35278

Report Number: CCEVS-VR-06-0059
Dated: January 26, 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

Table of Contents

Figure

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the HP Network Node Manager (NNM) Advanced Edition Software V7.51 with patch PHSS_35278.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

HP NNM is a network management system. It collects system data from across the targeted network, stores it in a database, and provides management capabilities. NNM also includes a capability to automatically set alarm thresholds for collected data based on deviations from historical data. If these thresholds are exceeded, then NNM will generate an alarm.

The Target of Evaluation (TOE) provides the following security features:

- Security Audit
- Security Management
- Data Collection, Analysis and Alarm Notifications
- Identification and Authentication
- User Data Protection (Access Control)
- Partial Protection of the TSF
- Partial Protected Data Transmission

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed during January 2007. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.2 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL2 from the Common Methodology for Information Technology Security Evaluation, Version 2.2, and Part 2: Evaluation Methodology [CEM]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives while countering specific threats.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4]. The Security Target (ST) is contained within the document Security Target for HP Network Node Manager Advanced Edition Software V7.51, v1.13 [ST]. The ST has been shown to be compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of CC.

2. Identification

Target of Evaluation:	HP Network Node Manager Advanced Edition Software V7.51 Advanced Edition with patch PHSS_35278
Evaluated Software:	HP Network Node Manager Advanced Edition Software V7.51 Advanced Edition with patch PHSS_35278
Developer:	Hewlett-Packard Development Company, L.P.
CCTL:	CygnaCom Solutions Suite 5200 7925 Jones Branch Drive McLean, VA 22102-3305
Validation Body:	NIAP Common Criteria Evaluation and Validation Scheme
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.2, Rev 256
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.2, Part 2: Evaluation Methodology

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.2 in the ST. A description of the principle security policies is as follows:

- **Data Collection, Analysis, and Alarm Notification**

  Data Collection

  NNM Server collects data from targeted network devices. NNM polls for the status of targeted network devices, network topology and configuration changes.

  Data Analysis

  NNM contains pre-defined event reduction configurations that present fewer alarms to the product's users. This capability is intended to identify common network problems and post a more meaningful alarm with all related alarms nested beneath. NNM also includes the capability to automatically generate alarms when a preset threshold is exceeded.

  Alarm Notification

Event-based alarms are displayed by the NNM's alarm browser capability. This capability is accessible via the Dynamic Views interface and allows the user to manage alarms stored in the database (e.g., display, filter, acknowledge, and delete).

- **Identification / Authentication and User Data Protection (Access Control)**

  The NNM server collects the identification and authentication information (username, password) from potential users of the Dynamic Views GUI. The NNM server maintains the user information and performs access control decision and enforcement. Additional factors in the access control decision are role assignment (NNM Administrator or NNM Operator) and whether the request is from the physical NNM server (local) vs remotely. The communication between the web browser and the NNM server is protected from modification or disclosure by the Secure Sockets Layer (SSL) protocol which is provided by the IT environment.

- **Security Management and Auditing**

  The NNM server provides the NNM Administrators with a command line interface (CLI) to perform most security management functions (e.g., . password setting, database setting, configuring the network behavior and customization). The capability to change their own password is available to NNM Administrators and Operators via the Dynamic Views Graphic User Interface (GUI). NNM server is responsible for creating and recording TOE audit records for security related audit events. The audit log is stored on the NNM server host and is viewable via the command line interface.

A summary of the SFRs for the TOE and IT environment are included in the tables below.

TOE Security Functional Requirements

Class FAU: Security Audit	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit Review
Class FIA: Identification & Authentication	
FIA_AFL.1	Authentication failure handling
FIA_SOS.1	Verification of secrets
FIA_UID.2-1	User Identification before any action
FIA_UAU.2-1	User authentication before any action
Class FMT: Security Management	
FMT_MTD.1-1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
Class CA: Collection and Analysis Requirements	
CA_SDC_EXP.1	System data collection

CA_ANL_EXP.1-1	Analyzer analysis
CA_ANL_EXP.1-2	Analyzer analysis
CA_RCT_EXP.1	Analyzer react
Class FDP: User Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
Class FPT: Protection of the TSF	
FPT_SEP_EXP_TSF.1	Partial TSF domain separation by the TOE
FPT_RVM_EXP_TSF.1	Partial Non-bypass ability of the TSP by the TOE.
Class FTP: Trusted path/channels	
FTP_TRP_EXP_TSF.1	Partial Trusted Path by TOE

IT Environment Security Functional Requirements

Class FAU: Security Audit	
FAU_STG.1	Protected audit trail storage
Class FDP: User Data Protection	
FDP_ACC.1-2	Subset access control
FDP_ACF.1-2	Security attribute based access control
Class FIA: Identification & Authentication	
FIA_UAU.2-2	User authentication before any action
FIA_UID.2-2	User identification before any action
Class FMT: Security Management	
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1-2	Management of TSF data
FMT_SMR.1-2	Security roles
Class FPT: Protection of the TSF	
FPT_RVM_EXP_PFM.1	Partial Nonbypassability of the TSP by the platform
FPT_SEP_EXP_PFM.1	Partial TSF domain separation by the platform
FPT_STM.1	Reliable time stamps
Class FTP: Trusted path/channels	
FTP_TRP_EXP_PFM.1	Partial Trusted Path by the IT environment

4. Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements.

ADO_DEL.1 Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

4.2 Environmental Assumptions

- It is assumed that TOE components are stored in a secure physical location to prevent unauthorized physical modification.
- Only trusted, knowledgeable, and authorized administrators will be able to manage, configure, operate, and access TOE, database and the underlying operating system according to the TOE documentation.
- No untrusted users will access the TOE or no untrusted software or data will reside on the TOE.
- TOE depends on the underlying operating system to provide user identification and authentication of root users accessing the TOE's CLIs, file protection, audit protection, and reliable time stamps.
- It is assumed that users will protect their authentication data.
- The TOE relies on the IT Environment to secure the network path between NNM server and web browser (requires the provided Tomcat/Apache software be configured to use SSL).

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:

1. This evaluation does not verify all claims made in the product's end-user documentation. The verification of the security claims is limited to those claims made in the TOE SFRs and TOE Summary Specification (see ST sections 5.2 and 6 respectively).
2. This evaluation only covers the evaluated configuration of the specific version identified in this document, and not any later versions released or in process.
3. As with all EAL2 evaluations, 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 ST provides additional information on the assumptions made and the threats countered.

5. Architectural Information

The evaluated product is the NNM Server which operates on the HP-UX 11.11 UNIX operating system platform. The Dynamic Views GUI is remotely accessed via a web browser (e.g., Internet Explorer on a Windows 2000 workstation). The NNM server

consists of the following components: NNM databases [embedded relational database and operational databases], NNM User Interfaces [Dynamic Views and CLI] and Syslog Agent. The product also includes two older GUIs that are NOT included in the TOE Boundary: Java GUI and Motif GUI. The following components in the IT environment are distributed with the product: Web server (Tomcat/Apache) and Java Runtime environment. See Section 2 of the ST for a full description.

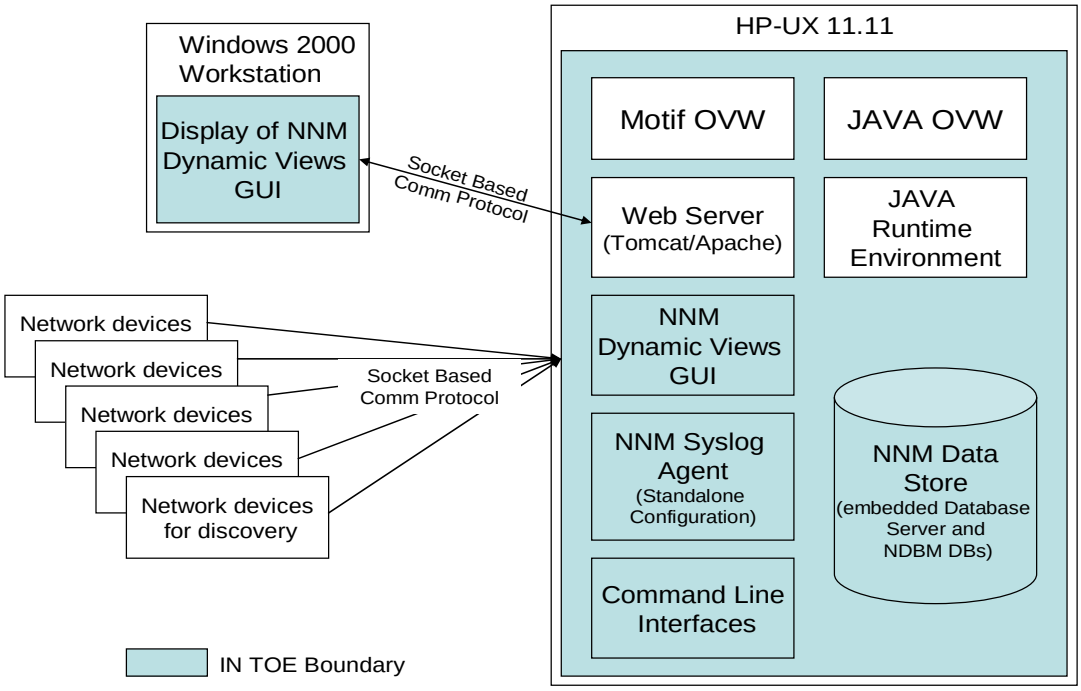

Figure1. TOE Physical Boundary.

6. Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- HP Network Node Manager Quick Start Installation Guide for HP_UX operating systems, dated May, 2006
- HP Network Node Manager Managing Your Network with HP Network Node Manager Windows, HP-UX, and Solaris operating systems, dated July 2004
- HP Network Node Manager Welcome to NNM Windows, HP-UX, and Solaris operating systems, dated July 2004
- HP Network Node Manager Using Extended Topology, dated July 2004
- HP Network Node Manager NNM Security Advisory Guide, dated November 16, 2006

7. IT Product Testing

At EAL2, the overall purpose of the testing activity is "to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST" (6.8 [CEM]).

At EAL 2, the developer's test evidence must only "demonstrate a correspondence between the tests and the functional specification" (ATE_COV.1, Evidence of Coverage [CC]) and does not include a test coverage analysis that shows that the "TSF has been tested against its functional specification in a systematic manner" (ATE_COV.2, Analysis of coverage [CC]). As a result, the developer's test evidence "need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested. Such shortcomings are considered by the evaluator during the independent testing sub-activity." (6.8.2.2 [CEM]).

The objective of the evaluator's independent testing sub-activity is "to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests" (ATE_IND.2, Independent testing – sample [CC]). The [CEM] provides the general guidance on the various factors that should be considered by the evaluators in devising their test subset and states that the "evaluators should exercise most of the security functional requirements identified in the ST using at least one test" (6.8.4.4 [CEM]). While, the evaluators build on the developer's testing and use the developer's correspondence evidence to identify shortcomings in the developer's test coverage, the evaluators do not perform a test coverage analysis that would demonstrates that all of the security functions as described in the functional specification were tested. As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

7.1 Developer Testing

The vendor testing covered the security functions identified in Section 6.1 of the ST. These security functions were: Audit, Data Collection, Analysis, and Alarm Notification, Security Management, Identification and Authentication, Partial protection of the TSF and Partial Protected Data Transmission.

The evaluator determined that the vendor tested most of the security-relevant aspects of the product that were claimed in the ST. The evaluator determined that the developer's tests were sound in their approach. The test document provided the configuration of the test hardware and software, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests. The evaluators determined that the developer's approach to testing the TSFs was appropriate for this EAL2 evaluation.

7.2 Evaluator Independent Testing

The evaluation team re-ran all of the developer tests and verified the results. The evaluation team then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

Test results, which are contained in proprietary reports, were satisfactory to both the Evaluation Team and the Validation Team.

7.3 Strength of Function

The TOE depends on the strength of the passwords used to authenticate access by its users. For authentication mechanisms a qualification of the security behavior can be made using the results of a quantitative or statistical analysis of the effort required to overcome the mechanism. The strength of function (SOF) requirement applies to the authentication mechanism (FIA_UAU.2-1). This mechanism is invoked for users accessing the TOE over the network interface using HTTPS to gain access to Dynamic Views. The TOE enforces a password policy that constrains passwords to a minimum of 8 characters with a mix of at lower case, upper case, numeric, and special characters (FIA.SOS.1). In addition, accounts are disabled and must be manually reset after 5 unsuccessful authentication attempts (FIA_AFL.1). The SOF metric of resistance of greater than 1 month to password guessing attacks applies for this authentication mechanism. A minimum SOF strength level claim for entire TOE is not applicable because the IT environment provides the authentication mechanism for users of the TOE's CLI functions.

7.4 Vulnerability Analysis

The developer searched for publicly known vulnerabilities specifically related to the TOE. No publicly-known vulnerabilities specific to the evaluated version of HP NNM V7.51 were found. The following public domain source was used to identify and search for relevant vulnerabilities:

- http://cve.mitre.org/cve

Known vulnerabilities in the IT environment could also be exploited to bypass the TOE's security policies. While these vulnerabilities are outside the scope of the evaluation, it is expected that the customer will installed the latest security critical patches to the operating system and database software. Under unusual circumstances a patch to TOE may also be required to address compatibility issues with a specific operating system or

database patch. The customer is advised check the HP support web site for any restrictions on specific patches to components of the IT environment.

The assumed level of expertise of an attacker is unsophisticated, with access to only standard equipment and public information about the product. The specific threats that the TOE is designed to counter are listed in section 3.2.1 of the ST.

8. Evaluated Configuration

The evaluated TOE is the HP NNM Advanced Edition Software version 7.51. New sealed installation disks were sent to the evaluator at HP Ft Collins.

Base product CDs labeled 7.50 for HP-UX (2 CD)
- Contains the README in an html form (interactive and multiple pages)
- Installation manual for the product in pdf form.
- Manpages for CLI

Upgrade CD labeled 7.51 for HP-UX (1CD)
- Contains the README in an html form (interactive and multiple pages)
- Installation manual for the product in pdf form.
- Manpages for CLI

Caution Note for HP-UX installation (only received when ordering NNM for HP-UX)

The patch PHSS_35278 can be downloaded by registered users from the HP web site (http://support.openview.hp.com/patches/nnm/nnm.jsp).

9. Results of Evaluation

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 version 2.2 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. 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 details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name

ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

10. Validator Comments/Recommendations

The Validation Team agreed with the conclusion of the CygnaCom CCTL Evaluation Team, and recommended to CCEVS Management that an EAL2 certificate rating be issued for the HP NNM V7.51.

11. Security Target

The Security Target is contained within the document Security Target for HP Network Node Manager Advanced Edition Software V7.51 with patch PHSS_35278, Version 1.13 [ST]. The ST is compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of the CC.

12. Glossary

The following table is a glossary of terms used within this validation report.

Acronym	Expansion
CC	Common Criteria [CC]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Criteria Evaluation Methodology [CEM]
CLI	Command Line Interface
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphic User Interface

IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NNM	Network Node Manager
OS	Operating System
PP	Protection Profile
SFR	Security Functional Requirement
SOF	Strength of Function
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation

13. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): http://www.nsa.gov/ia/industry/niap.cfm
- CygnaCom Solutions CCTL: http://www.cygnacom.com
- HP: http://www.hp.com

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.2, Part 2: Evaluation Methodology, January 2004.
- [CCEVS3] Guidance to Validators of IT Security Evaluations, Version 1.0, February 2000.
- [CCEVS4] Guidance to Common Criteria Testing Laboratories, Draft, Version 1.0, March 2001.

Other Documents

- [ST] Security Target for HP Network Node Manager Advanced Edition Software V7.51 with patch PHSS_35278, Version 1.13, January 11, 2007