National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

CA eHealth Suite Version 5.7 SP9

Report Number: CCEVS-VR-VID10267-2009

Version 1.0

28 January 2009

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

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

ACKNOWLEDGEMENTS

Validation Team

Jim Brosey
Orion Security Solutions

Daniel P. Faigin
The Aerospace Corporation

Common Criteria Testing Laboratory
Justin Fisher
Christopher Gugel
Amit Sharma
John Schroeder
Booz Allen Hamilton Common Criteria Test Laboratory
Linthicum, Maryland

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1 Executive Summary

The evaluation of the CA eHealth Suite Version 5.7 SP9 was performed by the Booz Allen Hamilton Common Criteria Test Laboratory in the United States and was completed on 5 January 2009. 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 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 2.3, for conformance to the Common Criteria for IT Security Evaluation, Version 2.3. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the CA eHealth Suite product by any agency of the US Government and no warranty of the product is either expressed or implied.

The Booz Allen Hamilton Common Criteria Test Laboratory evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met.

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

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

The technical information included in this report was obtained from the Evaluation Technical Report for the CA eHealth Suite v5.7 SP9 produced by Booz Allen Hamilton Common Criteria Test Laboratory.

2 Evaluation Details

Evaluated Product	CA eHealth Suite Version 5.7 SP9
Sponsor & Developer	CA Inc., Islandia, NY
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	28 January 2009
CC	*Common Criteria for Information Technology Security Evaluation*, Version 2.3, August 2005
Interpretations	None.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 2.3, August 2005
Evaluation Class	EAL 2
Description	The TOE is the CA eHealth Suite Version 5.7 SP9 software, which is a System, Application and Network Analysis and Reporting system developed by CA.
Disclaimer	The information contained in this Validation Report is not an endorsement of the eHealth Suite product by any agency of the U.S. Government, and no warranty of the eHealth Suite product is either expressed or implied.
PP	None
Evaluation Personnel	Justin Fisher Chris Gugel Amit Sharma John Schroeder
Validation Team	Jim Brosey Daniel P. Faigin

2.1 Interpretations

Table 1 provides a list of Interpretations applicable to this evaluation as of the kick off meeting held January 2008. These interpretations include:

Table 1 – Interpretations

PD-0086	What SOF Claim is appropriate when there are no probabilistic or permutational mechanisms
PD-0088	Developer Vulnerability Analysis
PD-0091	Dependencies of Requirements on the IT Environment
PD-0094	Site Visit - Alternative Evaluation Methodology
PD-0122	Description of Logical and Physical Boundaries

PD-0123	Defining Protocols as Internal or External Interfaces
PD-0124	Depth of Protocol or Interface Examination
PD-0129	Deletion of the oldest audit events when audit storage space is exhausted

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations.

2.2 Threats to Security

Table 2 summarizes the threats that the evaluated product addresses.

Table 2 – Threats

A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE. Unauthorized access could be granted via user error, system error, or other actions.
An administrator may incorrectly install or configure the TOE. This could result in a corrupted TOE that is ineffective in executing its security mechanisms.
Malicious users could attempt to misconfigure or modify their user accounts in an attempt to tamper with TOE resources or modify security information relative to the TOE.
A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
Users could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.
Users or network services could attempt to disable or degrade the performance of networks, systems or applications in the network.
Network devices which are unknown to the TOE could be added to the IT Environment and disable or degrade the performance of networks, systems or applications in the network.
Malicious users could monitor (e.g., sniff) network traffic.
A malicious user or process may compromise the cryptographic mechanisms and the data protected by those mechanisms to be inappropriately accessed (viewed, modified, or deleted).

3 Identification

The product being evaluated is the CA eHealth Suite Version 5.7 SP9.

4 Security Policy

4.1 Authorization

When users request access to resources protected by the TOE, their requests are assessed according to the eHealth discretionary access control policy. The eHealth Server checks the permissions set by the eHealth System Administrator for the End User account being accessed to determine which functions the user will be permitted to perform.

The eHealth Web server has secure access, which is enabled by default. Secure access requires users to log in using an eHealth Web user name and password. To allow a user to access the secure Web server and Web reports, the TOE administrator must create a Web user account for the user. After the TOE administrator enables Web security, administrative functions such as modifying user accounts, changing site configurations, or displaying access logs are available in the Authorized Access area. When the TOE Administrator clicks Authorized Access on the Administration page, he/she is prompted to specify a user name and password. The Authorized Access menu appears, and the TOE administrator can access the following administrative functions:

- Manage Users
- Access Logs
- Site Configuration
- Change Password
- Advanced Logging

4.2 Authentication

In the case of the Web Server Interface, the user initiates authentication to the web server component of the TOE using digest authentication from Apache; specifically, the Apache module mod_auth_digest controls the encryption of the passwords and protects the TOE from replay attacks. During the I&A process the system on behalf of the user performs the SSL protocol handshake. The user is then prompted with a login pop up window, and is allowed to enter I&A credentials. Authentication requires both a valid authentication attempt via SSL and a valid certificate exchange between the TOE (i.e., Apache Server) and the remote web browser.

The TOE maintains user identity, authentication data (I&A credentials), and authorizations on each user of the system. These take the form of the tuplet {username, password, group}. The username, group, and password are stored in the underlying operation system. The password is not stored in plaintext, but rather as a cryptographic hash. The Identification and Authentication function stores the user's associated role, which essentially takes the form of the couplet {username, group}.

A user must authenticate to the eHealth Suite to perform any action on the TOE. The information is sent encrypted via HTTP over SSL, as described above, from the user's web browser to the eHealth Suite where access is either granted or denied.

4.3 Audit

The TOE produces audit data (i.e., access logs) to track all users interaction with the TOE through the Web Server component of the TOE, including password changes, generation of reports, and viewing reports.

The TOE relies upon the underlying OS to store the audit data generated by the TOE.

Using the Access Logs option in the Site Management area of the Administration page, eHealth System Administrators can generate (a) a detailed list of all connections that all or specific End Users have made to the eHealth Suite, (b) all or specific Web pages that End Users have

accessed, and (c) a specific time and date range during which the access occurred. In addition, the eHealth System Administrator can also display summary statistics of individual connections to the eHealth Suite (that is, for each report page). Figure 1 describes the report details and page statistics that can be obtained by generating an access log.

Figure 1 – Access Log Attributes

Report Details	Individual Page Statistics
• Time range during which user(s) accessed the Web server • Name of user(s) who accessed the Web server • Type of report page that the user(s) accessed • Workstation IP addresses from which the user(s) performed the operation • Total number of operations performed	• IP address of workstation from which the page was accessed • Web user account name(s) • Date and time at which the page was accessed • Name of the operation that was performed (for example: GET or POST) • Pathname of the page that the user (s) visited • Return code • Total amount of data (in bytes) that was transferred

The TOE calls these logs audit files Access logs in the user GUI, they are synonymous with standard Apache web logs. The log files specifically are:

1. **Web Server Log httpd-log.** Standard Apache web log of all HTTP requests, including user login, password changes, report generation, and viewing of reports.
2. **Web Server Log httpd-error.** Standard Apache web log errors resulting from HTTP requests.

4.4 Security Management

Security Management is implemented by the TOE through interactions by the administrator from a Remote Workstation and locally on the TOE via the X Windows (Motif) console. For remote access the administrator logs into the eHealth Suite via an SSL enabled web browser. Once authenticated, the administrator has access to security management tabs within the eHealth Suite software that enable him/her to control system access by others. The administrator can control the data objects that users may generate reports about or view. Additionally, the administrator may manage the login attributes of the End Users. From the Motif console the local administrators can manage user accounts, groups, and grouplists; view the system message logs, schedule jobs and manually run the discover process.

In the evaluated configuration, the Motif console is used solely for the Discover and polling processes. Once elements are discovered and are polled, users of the TOE will interact with the Web GUI to run reports based on the outcome of the polling process. While the Motif console has a variety of functions, running the Discover process is the only Motif activity within the scope of the evaluated configuration.

The following three bullets capture at a high-level the security management functions of the TOE (for additional detail please refer to section 6.1.5 of the Security Target):

- (Managing User Accounts Using Groups and Group Lists) Elements may be collected together via objects known as groups, and the groups in turn in to group lists. These form not only fundamental domain-level collection facilities, but also for the basis for access control among multiple users.
- (Changing User Passwords) The TOE administrator can add new users and set their permissions. The TOE administrator can add, modify, and delete user and system passwords for all users. Other users can modify only their own passwords.
- (Providing Access to Groups and Reports) As the TOE administrator, it is possible to grant users permissions to view and use none, some, or all groups and group lists. For example, Internet Service Provider (ISP) operators need to see a group list that contains all of their customers. However, they would likely create a group for each customer and restrict access so that each customer views only their own activity. Groups and group lists also restrict which eHealth reports can be run by a user.

4.5 Trusted Path/Protection of the TSF

The protection mechanisms employed by the TOE ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. More specifically, once a user has been authenticated via Web interface, the Identification and Authentication function is used to query and return the user's role. The role is used to determine the functionality that is presented to the user. For the Application TOE, the host IT environment administrator can access the TOE to change the time and halt the execution of the application. Because the host IT environment is considered to be a trusted IT entity and the interface established to change the time and halt the TOE is via a trusted path, the security domain for the Application TOE is still considered protected from interference and tampering. A trusted path is established for all user communication between the TOE and the remote administration console via HTTP over SSL. No other means, other than described above, are provided for the user to interact with the TOE. The use of SSL ensures that all traffic to and from the TOE via the remote administration interface is protected from unauthorized disclosure. The passwords are not sent in the clear but use an MD5 hash for comparison to a shared secret on the TOE. All SSL data is encrypted with a 3DES and RSA is used for symmetric key exchange.

4.6 Self Protection

The self-protection function is responsible for providing an execution domain that is protected from interference and tampering by unauthorized users. The TOE is an application running on a dedicated device that executes all of its processes internally. It is accessible only via the defined interfaces; and only authorized users and the host IT environment for the TOEs are able to modify the functionality of the TOE. The poller interface enforces domain separation in that any data sent to this interface (which is presumed untrusted) is logically separated from all other TOE data. All data sent to the Poller interface is never executed but rather is parsed for analysis. Traffic flowing through the TOE is subject to the policies as defined by the authorized users. At all physical interfaces, the TOE intercedes to ensure domain separation. Traffic can only come

into the TOE via four physical interfaces: the local CLI interface (which is used only during initial setup and configuration of the TOE), the network interface (access to which is controlled by a username and a password), the Oracle Database (which is only accessible by internal TOE processes) or the poller interface (where the traffic is monitored and analyzed by the TOE but no actions can be executed). Traffic and/or unauthorized users cannot bypass the identification and authentication mechanisms, preventing interference and tampering by untrusted subjects and thereby maintaining a domain for its own execution. The self protection function of the Module TOE and the self protection features of the host IT environment work together to satisfy the self protection requirements. The reliable time value is received upon boot up or modified via a trusted channel from the host IT Environment. The host IT Environment mediates its interfaces to only allow authorized modifications while protecting those interfaces from interference and tampering. For example, once the clock is initialized or modified via the trusted interface the IT Environment ensures those interfaces are free from interference and tampering.

5 Assumptions

5.1 Personnel Assumptions

Table 3 – Personnel Assumptions

One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains in order to maintains its security objectives.
All users of the TOE are properly trained in the configuration and usage of the TOE and will follow the guidance provided.
eHealth System Administrators will properly patch the IT Environment in a manner that maintains its security objectives.
Users will select strong passwords according to the policy described in the administrative guidance and will protect their authentication data.

5.2 Physical Assumptions

Table 4 – Physical Assumptions

Those responsible for the TOE must ensure that the TOE hardware and software critical to security policy are protected from physical attack and unauthorized physical modification, which might compromise the TOE security objectives.

5.3 Logical Assumptions

Table 5 – Logical Assumptions

The monitored network is isolated and safe from interference by other networks.

6 Clarification of Scope

The TOE includes all the code that enforces the policies identified (see section 4). The TOE also includes secure communications functions; i.e., HTTP over ssl (openssl v9.7d).

The evaluated configuration of the TOE includes the CA eHealth Suite v5.7 SP9 application that is comprised of the following:

- Sun SunBlade 1500 running Solaris 2.9
- UltraSPARC-IIIi, 1062 MHz CPU
- 4 GB memory
- 140 GB Diskdrive
- eHealth Version 5.7 Service Pack 9
- Apache Web Server v1.3.31 (included in eHealth) with Apache SSL plug-in (from CA Technical Support) installed and configured.

The evaluated configuration does not include the following features described in the user manual:

- Command line features. It is assumed that access to commands is within the OS security perimeter.
- Database areas. It is assumed that access to the Oracle database is within the OS security perimeter.
- SystemEDGE security testing.
- Live Health.
- OneClick for eHealth (OCE) security testing. OCE is an optional add-on offering.
- TrapEXPLODER security testing.
- Detection of Denial of Service attacks.

The scope and requirements for the evaluated configuration are summarized as follows:

1. The eHealth Suite Version 5.7 SP9 software (i.e., the TOE) will be installed on the eHealth Server machine with the Solaris 2.9 operating system installed.
2. The Oracle 9i Database, base version 9.2.0.3, will communicate with the eHealth Suite Version 5.7 SP9 software and will be installed on the eHealth Server machine.
3. The Oracle listener presents a security vulnerability and is not used by eHealth. The Common Criteria installation guidance requires that the ORACLE listener be disabled.

6.1 System Requirements

This section identifies the hardware and software requirements for the platforms described in the evaluated configuration. The TOE was evaluated in on a UNIX platform only. This configuration is detailed in the following subsection.

6.1.1 eHealth Server UNIX Platform

For the evaluated configuration on the UNIX platform, the operational TOE runs on the following hardware device:

- Sun SunBlade 1500 running Solaris 2.9
- UltraSPARC-IIIi, 1062 MHz CPU
- 4 GB memory
- 140 GB Diskdrive

6.1.2 Remote Workstation Platform

For the evaluated configuration of the TOE, the Remote Workstation can be any standard Windows or UNIX workstation that includes a web browser from the following list:

- Mozilla Version 1.2.1 or later (UNIX)
- Internet Explorer Version 6.0 or later (Windows)
- Netscape Communicator Version 7.1 or later (Windows)
- Mozilla Version 1.6 or later (Windows)

6.2 Physical Boundary Components

Section 6.2.1 (Hardware Components) and section 6.2.2 (Software Components) denote the components that are in the TOE and that are in the environment.

6.2.1 Hardware Components

Table 6 identifies hardware components and indicates whether or not each component is in the TOE.

Table 6 – Hardware Specifications

TOE or Environment	Component	Description
Environment	eHealth Server UNIX Platform	Sun SunBlade 1500 running Solaris 2.9 UltraSPARC-IIIi, 1062 MHz CPU 4 GB memory 140 GB Diskdrive
Environment	Remote Workstation Platform	Any standard Windows or Unix workstation, running an approved web browser with javascript enabled Specific version numbers are specified in the Software Components section.

6.2.2 Software Components

Table 7 identifies software components and indicates whether or not each component is in the TOE.

Table 7 – Software Specifications

TOE or Environment	Component	Description
TOE	eHealth Suite Version 5.7 SP9	Software package installed includes all TOE items listed below: Poller Processes eHealth Processes Apache Web Server v1.3.31 with mod_SSL.
Environment	Solaris 2.9	eHealth Operating System
Environment	Oracle 9i Database	Oracle Database, update 9.2.0.3
Environment	Web Browser	Remote Web Browser with javascript enabled UNIX systems: Mozilla Ver. 1.2.1 or later Windows systems: Internet Explorer Ver. 6.0 or later, Netscape Ver. 7.1 or later, and Mozilla Ver. 1.6 or later

The installation and configuration of the TOE and the Operational IT Environment were performed as described in the installation guidance, and meet all boundary requirements of the ST.

7 Architectural Information

The self-protection function of the TOE is responsible for providing an execution domain that is protected from interference and tampering by unauthorized users. The TOE is an application running on a dedicated device that executes all of its processes internally. It is accessible only via the defined interfaces and only authorized users and the host IT environment for the TOE are able to modify the functionality of the TOE. The poller interface enforces domain separation in that any data sent to this interface (which is presumed untrusted) is logically separated from all other TOE data. It is never executed but rather is parsed for analysis. Traffic flowing through the TOE is subject to the policies as defined by the authorized users. At all physical interfaces, the TOE intercedes to ensure domain separation. Traffic can only come into the TOE via four physical interfaces: the local CLI interface (which is used only during initial setup and configuration of the TOE), the network interface (access to which is controlled by a username and a password), the Oracle Database (which is only accessible by internal TOE processes) or the poller interface (where the traffic is monitored and analyzed by the TOE but no actions can be executed). Traffic and/or unauthorized users cannot bypass the identification and

authentication mechanisms, preventing interference and tampering by untrusted subjects and thereby maintaining a domain for its own execution. The reliable time value is received upon boot up or modified via a trusted channel from the host IT Environment. The host IT Environment mediates its interfaces to only allow authorized modifications while protecting those interfaces from interference and tampering.

7.1 Logical Boundary

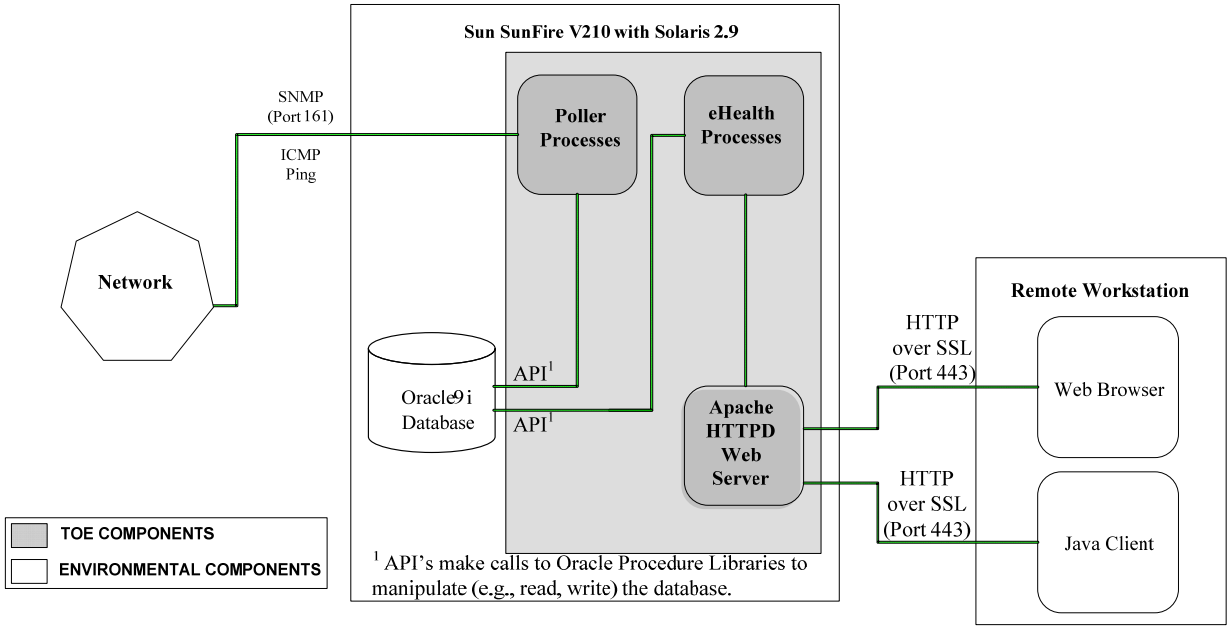

Figure 2 – TOE Logical Boundary

The logical boundary of the TOE includes the eHealth Suite Version 5.7 SP9 Server software. This component enforces Authorization, Authentication, Audit, Data Protection, and Security Management as described in the following subsections.

7.1.1 Authorization

eHealth Suite Authorization protects the server resources from unauthorized access. An End User's capability of accessing pages and files, and running applications or reports are controlled by the corresponding authorization policy.

Access privileges granted to users are managed by the eHealth application. The eHealth application stores the user privilege information on a CSV file on the operating system where eHealth runs. When a user requests content from the eHealth application, the eHealth application validates the authorization to this content by comparing the validated username provided by the web server with the list of access rights on the Authorization database (CSV). For database access, the eHealth application verifies that the OS user has access to the Oracle database and grants it DBA rights. Additional accounts are granted read only access rights.

The eHealth admin has the privileges associated with the eHealth account created and maintained by the underlying Operating System (i.e., Solaris 2.9). This account will have access to the various files used by the TOE and stored and protected by the underlying OS.

7.1.2 Authentication

Authentication services are handled internally through passwords. eHealth Authentication is the process of determining the End User's true identity and mapping them to the appropriate role (i.e., eHealth administrator or End User). This is enforced by the TOE. Authentication through remote access is the only allowed access to the TOE in its operational configuration. The end users identity and password is maintained in a web server configuration file stored on the local Solaris file system.

A remote workstation will use an authorized web browser (see section 6.1.2) to interact with the TOE via the SSL Web interface port 443 to the Apache Web Server. A username and password request is issued by the web server. The user provides a username and password to the web server, which is passed to the eHealth server via an industry standard web browser, see section 6.1.2 for the supported web browsers. The Apache web server validates the users claimed credentials against password and usernames stored in a web server configuration file stored on the local file system. The TOE returns the success or failure of the authentication process. If properly authenticated, the web server provides the username that has been authenticated to the eHealth application. TOE passwords are stored locally on the operating system in their hashed form (MD5). When a user presents their password to the TOE, it is also hashed with MD5 and the two hashes are compared. If the hashes match then access is allowed.

7.1.3 Audit

The TOE generates audit records for selected security events. Events are tracked based on occurrence and who triggered them. Results are recorded to a local log text file on the eHealth Server that is stored and protected by the host Operating System. Logins can be audited via log files prepared by the web server, and displayed to the privileged (administrative user) via the web interface. This login log file is also protected and stored on the host Operating System. As a result, the eHealth System Administrator can utilize the contents of the log files for further processing. A web browser in the TOE environment is required to read the audit records. The eHealth System Administrator interacts with the TOE from a Remote Workstation. The eHealth System Administrator is required to successfully identify and authenticate themselves to the TOE before being granted permission to review the generated audit information.

7.1.4 Data Protection

The access control features of the underlying operating system protect all the TOE data. Local access is not permitted by any user other than an authorized IT environment administrator that has an account on the local machine. End Users log on to the machine via a Remote Workstation, and are not permitted to edit any of the information stored on the eHealth Server.

7.1.5 Protected Data Transmission

The TOE uses an Apache web-server to support protection of external TOE communication with the users by performing SSL encryption through Apache's OpenSSL-based cryptographic module (mod_SSL). The TOE uses openssl v9.7d. The protocol for transport is HTTP over the Secure Socket Layer protocol, sometimes referred to as "HTTPS" or "HTTP over SSL." HTTP over SSL can be used as the secure communication between the eHealth server and the remote workstation. The eHealth server relies on the user's web browser in the IT environment to

perform the SSL protocol with its associated cryptography to process certificates for authenticating the end points of the communication channel and to encrypt the data.

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

7.1.6 Partial TOE Self Protection

The TOE works with the IT environment (OS and DB) to provide protection of its security functions through non-bypassability and domain separation. All user operations are conducted in the context of an associated session. The TOE manages these sessions to prevent one session from compromising another session. The TOE provides only well-defined interfaces to these sessions, and the sessions allocated only after successful authentication, or when a session is requested from the physically protected local console, which is under procedural control. The TOE relies on its platform to operate correctly and to prevent unauthorized access to TOE data and stored executables.

7.1.7 Security Management

Security Management is handled by an authorized eHealth Systems Administrator via the Remote Workstation. Access to the Security Management user interface is secured by the core operating system authentication scheme and role based permissions. Administrators are permitted to edit user account attributes and access permissions while end users are denied these privileges.

8 Documentation

The following documents were evaluated per assurance requirement. Publically available documents are **bolded and underlined**.

Table 8 – Assurance Documents Evidence

Component	Document(s)
Configuration Management (ACM)	[1] Build and Kitting Windowsv2.0 [2] eHealth Nightly Builds (UNIX)v2.0 [3] NVM IT Backup Strategy v1.1 [4] NVM Source Code Best Practices v1.1 [5] New eHealth Checkin Process Rollout for eHealth Suite Version 5.7 version 2.0 [6] Configuration Item List.txt **[7] CA eHealth 5.7 SP9 Delivery**
Delivery and Operation (ADO)	**[1] Concord Communications Software Delivery Procedures, Version 1.0** **[2] CA eHealth 5.7 SP9 Delivery** **[3] Installation GuideUNIX57 (MN-INSTALUN-003)** **[4] eHealth Installation Addendum for UNIX (r5.7)** **[5] eHealth+SSL+SiteMinder**
Development (ADV)	[1] Functional Specification Document for CA eHealth v 5.7 SP9 v1.2 **[2] eHealth Administration Reference (MN-EHADMREF-002)** **[3] eHealth Web Administration Guide (MN-EHWEBADM-001)** **[4] eHealth Administration Guide (MN-EHADMGD-002)** **[5] eHealth Installation Guide: New Installations (UNIX) (MN-INSTALUN-003)** **[6] Querying the Database Using the DB API (MN-DBAPI-002)** **[7] Introduction to eHealth (MN-INTROEH-002)** [8] eHealth Web Help Contents v5.7 [9] High Level Design Document for CA eHealth v 5.7 SP9 v1.3
Guidance Documents (AGD)	**[1] Computer Associates eHealth Suite Version 5.7 Admin Supplemental Guidance, v1.0** **[2] eHealth Web Administration Guide (MN-EHWEBADM-001)** **[3] eHealth Administrator Guide (MN-EHADMGD-002)** **[4] eHealth Administration Reference (MN-EHADMREF-002)** [5] eHealth Web Help Contents v5.7
Tests (ATE)	[1] eHealth Security Version 5.7 Test Plan v1.0 [2] eal_security_pts_57.xls
Vulnerability Assessment (AVA)	**[1] Computer Associates eHealth Suite Version 5.7 Admin Supplemental Guidance, v1.0** **[2]** CA eHealth Suite v5.7 SP9 Vulnerability Analysis v1.1

9 TOE Acquisition

The NIAP-certified eHealth product is acquired via normal sales channels, and digital delivery of the TOE is coordinated with the end customer by CA.

10 IT Product Testing

The evaluators test approach was to test the security mechanisms of the Computer Associates eHealth 5.7 SP9 by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface was described in Computer Associates design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, High-Level Design (HLD), Functional Specification (FSP), and the vendor's test plans were used to demonstrate test coverage of all EAL2 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that were determined to be *security relevant* are interfaces that do one or more of the following:

- Change the security state of the product
- Permit an object access or information flow that is regulated by the security policy
- Are restricted to subjects with privilege or behave differently when executed by subjects with privilege
- Invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

The evaluation team created a test plan that contained a sample of the vendor functional test suite, and supplemental functional testing of the vendor's tests. Booz Allen also performed vulnerability assessment and penetration testing.

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

10.1TEST METHODOLOGY

The evaluation team used 11 different types of tests. They included the following:

Table 9 – Tests Performed

Test Number	Test	Objective
1	Eavesdropping on Communications	The evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful information could be obtained by a malicious user on the network.
2	Unauthenticated Access / Directory Traversal / CGI Exploitation	This test included three different methods of URL exploitation 1. The first part of this test attempted to access protected TOE resources as an unauthenticated outsider. 2. The second part of the test attempted different methods to access local TOE resources that should be protected from any remote access (unauthenticated and authenticated). 3. The third part of the test attempted to access protected

		resources on the TOE through any potential CGI vulnerabilities
3	Port Scanning - Remote access to the TOE should be limited to the standard TOE interfaces and procedures.	This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
4	Direct Database Access - The TOE should perform all direct interaction to and from the backend database.	This test attempted to access the backend database directly and bypass the normal access procedures.
5	Web Server Vulnerability Scanner	This test used the Nikto web server vulnerability scanner to test for any known vulnerabilities that could be present in the TOE's web interface. This scanner probed a wide range of vulnerabilities that included the following: • File Upload. • Interesting File / Seen in logs. • Misconfiguration / Default File. • Information Disclosure. • Injection (XSS/Script/HTML). • Remote File Retrieval • Denial of Service. • Remote File Retrieval • Command Execution / Remote Shell. • SQL Injection. • Authentication Bypass. • Software Identification • Remote source inclusion.
6	Generic Vulnerability Scanner	This test used the Nessus Vulnerability scanner to further test not only the web interface of the TOE, but also any other interface that is present. This scanner probed a wide range of vulnerabilities that included the following: • Backdoors • CGI abuses • Denial of Service • Finger abuses • Firewalls • FTP • Gain a shell remotely • Gain root remotely • General • Miscellaneous • Netware • NIS • Port scanners

		• Remote file access • RPC • Settings • SMTP Problems • SNMP • Untested • Useless services
7	Buffer Overflow / Cross Site Scripting / SQL Injection	This test performed automated buffer overflow, cross site scripting, and sql injection attacks against the TOE as both an authenticated and an unauthenticated user.
8	Hijack SNMP Session	This test attempted to corrupt the state of the TOE by effectively taking over a session between the eHealth server and a polled device. If successful, the TOE would be given false information about the device and potentially report it as true.
9	Denial of Service	This test attempted to exploit a known vulnerability using nonstandard input to the TOE that would, in theory, prevent its normal functionality.
10	Certificate Integrity	This test demonstrated the claimed functionality of the TOE to overwrite and change encryption keys.
11	ICMP Blind Connection Reset	This test attempted to exploit a known vulnerability using ICMP connection reset packets. If effective, this test would prevent the normal functionality of the TOE and invoke a denial of service against it.

11 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the CA eHealth Suite v5.7 SP9 TOE meets the security requirements contained in the Security Target.

The criteria against which the CA eHealth Suite v5.7 SP9 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the CA eHealth Suite v5.7 SP9 TOE is EAL 2. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed in January 2009. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

12 Validator Comments/Recommendations

During the evaluation of the product there were some noteworthy observations as follows:

1. The evaluated product does not provide additional protections for audit data files or other logs. The records of the TOE are being protected by the OS, which is an environmental component. One has to have OS account to be able to log in and access the files. The security would be as vulnerable as the Operating System on which eHealth runs. Gaining unauthorized access to the root/administrator account or to any of the authorized eHealth accounts will grant the user access to all the data provided by the interface.
2. eHealth does not pose requirements for strong passwords. The responsibility of issuing strong passwords is levied upon the operating organization. An example of a strong password policy follows:
   - At least 8 characters long
   - Does not contain your account or full name
   - Contains at least 3 of the following 4 character groups: English uppercase characters; English lowercase characters; Numerals (0 through 9); Non-alphabetic characters (such as !, $)

   Note that this may have impact on the ability of systems integrating the TOE in a DoD environment to satisfy the DODI 8500.2 IAIA control.
3. A cross site scripting vulnerability was discovered during testing. This vulnerability is not addressed in eHealth v5.7. Its recommended that the administrator warn users that if they are interacting with eHealth but the browser has a suspicious URL (i.e. one that differs from the original hostname and/or is extremely long) they should exit eHealth and start a new session. The vendor asserts that this vulnerability has been addressed and does not exist in eHealth v6.1.
4. The TOE uses SNMP protocol “version 1”. SNMP v1 has a number of reported vulnerabilities that could be exploited if not deployed in an isolated network environment.
5. The web component of the TOE runs on top of TCP, which is known to be vulnerable to several denial of service attacks that could allow an attacker to reset a TCP connection. Such attacks are byproducts of the protocol itself and are not caused in the TOE.
6. When installing and configuring the TOE, refer to the delivery documentation. Section 3 of this document includes the installation steps which need to be performed. The last step of this references the supplemental administrative guidance. This guidance contains additional information that administrators should be aware of and also contains configuration instructions that will help mitigate threats. The TOE must be configured as described in these documents to operate in a secure state. Failure to do so may make the overall system subject to vulnerabilities.
7. The TOE can be managed via IP address, but if using DNS, it is the organization’s responsibility to ensure that the DNS is trusted.

8. It is the organization's responsibility to configure Apache as described in the eHealth installation instructions. Failure to do so may make the overall system subject to vulnerabilities. This evaluation did not check whether or not the TOE would function correctly if Solaris was configured in accordance with the Unix STIG and the underlying Oracle database was configured in accordance with the Database STIG.
9. Vulnerability CVE-2007-1349, a mod_perl denial of service vulnerability, is exploitable in the TOE, but only by a Medium level attack. This is an acceptable residual vulnerability since this product was only evaluated against a low-level attack potential. This vulnerability needs to be considered if protection against medium level attacks is required.
10. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

13 Annexes

Not applicable.

14 Security Target

The security target for this product's evaluation is *CA eHealth Suite Version 5.7 SP9 Security Target, Version 2.4, 2009-01-27*

15 List of Acronyms

CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
CEM	Common Evaluation Methodology
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
EAL	Evaluation Assurance Level
IT	Information Technology
NTP	Network Time Protocol
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function

SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol

16 Terminology

eHealth System Administrator: The eHealth System Administrator is empowered to configure the eHealth Suite, monitor deployment, user accounts and settings, and reporting options within the software. The eHealth System Administrator is assigned when the eHealth Server is initially installed and set up.

End Users: Refer to the individuals for whom web accounts have been set up on the eHealth Suite by the eHealth System Administrator. These users can view network node system settings, generate reports, and view other settings dependent upon the privileges assigned to them by the eHealth System Administrator.

17 Bibliography

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

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

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

[4] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, Version 2.3.

[5] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, Version 2.3.

[6] CA eHealth Suite Version 5.7 SP9 Security Target, Version 2.4, 2009-01-27

[7] CA eHealth Suite Version 5.7 SP9 Evaluation Technical Report (ETR), Version 1.1, 2009-01-28

[8] Evaluation Team Test Plan for the CA eHealth Suite Version 5.7 SP9, Version 1.0, 2008-12-29