National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Guidance Software EnCase® Enterprise V6.8

Report Number: CCEVS-VR-VID10052-2008
Dated: 20 November 2008
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

List of Tables

1 Executive Summary

The evaluation of the Guidance Software EnCase® Enterprise V6.8 product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in June 2008. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 2.3. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

The SAIC evaluation team determined that the product is Common Criteria Part 2 Conformant and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 2. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

EnCase Enterprise is designed for corporate and government organizations that need the ability to perform internal computer investigations of all types. It establishes an investigative infrastructure that provides network-enabled search, identification, preservation, analysis and reporting of digital evidence on employee computers and file servers for the purposes of internal investigations such as fraud, HR matters and computer incident analysis and response. The solution views data at the binary level, providing the capability to find hidden files such as rootkits and identify zero-day exploits. In addition the software provides the ability to remediate malicious processes, and serves as a platform for add-on data discovery capabilities (not included in the evaluated configuration) for the purposes of sensitive data auditing and eDiscovery.

The evaluated functionality of the TOE comprises: the user data protection function that controls what operations users can perform during the course of an investigation; security management of the TOE, its users, and the access control policy; auditing of security management and access control operations; identification and authentication of users; and cryptographic support for protection of TSF and user data.

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	Guidance Software EnCase® Enterprise V6.8
Sponsor:	Guidance Software, Inc. 215 North Marengo Avenue, Second Floor Pasadena, CA 91101
Developer:	Guidance Software, Inc. 215 North Marengo Avenue, Second Floor Pasadena, CA 91101
CCTL:	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046

Kickoff Date:	November 19, 2004
Completion Date:	October 7, 2008
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 2.3, August 2005.
Evaluation Class:	EAL 2
Description:	EnCase Enterprise allows organizations to perform internal computer investigations. It supports network-enabled search, identification, preservation, analysis and reporting of digital evidence on computers and file servers for the purposes of internal investigations and computer incident analysis and response.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Guidance Software EnCase® Enterprise product by any agency of the U.S. Government and no warranty of the Publisher product is either expressed or implied.
PP:	None
Evaluation Personnel:	Science Applications International Corporation: Anthony J. Apted Katie Sykes Quang Trinh
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE is intended to counter.

T.ACCESS Users may gain access to the functions of the TOE to which they are not authorized.

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.TRANSIT	An unauthorized user may eavesdrop on communications between separate parts of the TOE allowing them to intercept and modify transmitted information

2 Identification

The evaluated product is **Guidance Software EnCase$^{®}$ Enterprise V6.8.**

3 Security Policy

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the EnCase Enterprise security policy has been extracted and reworked from the Guidance Software EnCase$^{®}$ V6.8 ST and Final ETR.*

3.1 Security Audit

EnCase Enterprise generates log files of the transactions that occur at the SAFE. Audit logs include information for each audited event, including the identity of the responsible user. EnCase Enterprise offers the ability for authorized administrators to perform an audit log review.

3.2 Cryptographic Support

The TOE cryptographic capabilities are provided by the EnCase Enterprise Cryptographic Module 1.0, which is a FIPS 140-2 validated cryptographic module (certificate #942).

3.3 User Data Protection

EnCase Enterprise restricts access to the network resources (target nodes) based upon the role assigned to the user.

3.4 Identification and Authentication

EnCase Enterprise ensures users are identified and authenticated prior to allowing them the ability to access its security functions. Users are identified with a user name and authenticated with a password. User attributes include user name, authentication data (password), role, permissions, and permitted node IP addresses.

3.5 Security Management

EnCase Enterprise provides two security management roles: Keymaster; and administrators. EnCase Enterprise provides the Keymaster and authorized administrator with a graphical user interface (GUI) that can be used to configure and modify EnCase Enterprise options. There are several modules available to the Keymaster and authorized administrator, such as manage user accounts and modify the behavior of the Access Control Policy. EnCase Enterprise restricts the ability to modify the behavior of security functions to the Keymaster and authorized administrators.

3.6 Protection of the TSF

As a product that is inherently distributed across a network, information passed between separate parts of EnCase Enterprise are encrypted to ensure that information is neither intercepted nor modified between two parts of the system. In addition, EnCase Enterprise ensures that the security enforcement functions are both invoked and successful before each function within EnCase Enterprise's scope of control is allowed to proceed.

4 Assumptions

The following assumptions are identified in the ST:

Table 2 – Assumptions

Assumption Identifier	Assumption Description
A.PROTECT	The components of TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.
A.TIME	The TOE's IT environment will provide a reliable time source to enable the TOE to timestamp audit records
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4.1 Clarification of Scope

The Target of Evaluation (TOE) is Guidance Software EnCase® Enterprise V6.8.

The TOE is dependent on the IT environment for provision of separate secure execution domains for each of the TOE components, and for the provision of reliable date/time stamps. Furthermore, the intended method of use in the evaluated configuration is for investigators to remotely connect to Servlets via the SAFE, rather than to launch investigations of the local machine on which the Examiner component is installed.

5 Architectural Information

The Target of Evaluation (TOE) is Guidance Software EnCase® Enterprise V6.8.

EnCase Enterprise is designed for corporate and government organizations that need the ability to perform internal computer investigations of all types. It establishes an investigative infrastructure that provides network-enabled search, identification, preservation, analysis and reporting of digital evidence on employee computers and file servers for the purposes of internal investigations such as fraud, HR matters and computer incident analysis and response. The solution views data at the binary level, providing the capability to find hidden files such as rootkits and identify zero-day exploits. In addition the software provides the ability to remediate malicious processes, and serves as a platform for add-on data discovery capabilities (not included in the evaluated configuration) for the purposes of sensitive data auditing and eDiscovery.

EnCase Enterprise has three main components that are installed separately. The components that comprise the TOE are the Secure Authentication For EnCase (SAFE), the Examiner, and the Servlet:

- **SAFE** (Secure Authentication For EnCase)—the SAFE is the software component that is used to authenticate administrators, administer access rights, retain logs of EnCase Enterprise transactions, broker communications, and provide for secure data transmission. The SAFE communicates with Examiners and targeted Servlets using encrypted data streams, ensuring no information can be intercepted and interpreted.
- **Examiner**—the Examiner is the system used by authorized administrators to perform incident response, investigations, and audits on designated systems.
- **Servlet**—the Servlet is the agent software that is installed on targeted workstations and servers. The Servlet allows the SAFE and the Examiner to preview, acquire and analyze volatile and static data residing on targeted machines.

The SAFE provides the following security functionality:

- Identification & Authentication—the SAFE identifies and authenticates users prior to allowing them to perform investigative or administrative operations
- User Data Protection—the SAFE associates users with roles that support investigative operations and that are subject to the TOE’s Access Control Policy. The SAFE determines if a user’s role has the necessary privilege to allow them to request a particular investigative operation from the Servlet, and that the user is authorized to access a target machine based on the target’s IP address
- Security Management—the SAFE implements the security management functions that allow administrators to manage users, their security attributes and the operation of the access control policy by determining the permissions that define user roles and by associating users with roles and authorized IP addresses
- Auditing—the SAFE generates audit records of the following events: failed and authorized authentication events; user creation and modification; successful and failed access control attempts, including connecting to Servlets; running snapshots; starting and stopping the SAFE service
- Cryptographic Support—the SAFE generates the symmetric session keys used to protect communication between the Examiner and Servlet, and performs digital signature generation and verification when authenticating itself to Examiners and Servlets
- TSF Protection—the SAFE ensures no functions can be invoked unless and until it has identified and authenticated the requestor.

The Examiner provides the following security functionality:

- Cryptographic Support—the Examiner provides the capability to: generate public-private keypairs for user accounts; encrypt and decrypt data transmitted between the Examiner and a Servlet, using the symmetric session key provided by the SAFE; performs digital signature generation and verification when authenticating to the SAFE

The Servlet provides the following security functionality:

- Cryptographic Support—the Servlet: encrypts and decrypts data transmitted between the Servlet and an Examiner, using the symmetric session key provided by the SAFE; performs digital signature generation and verification when authenticating to the SAFE.

6 Documentation

The guidance documentation examined during the course of the evaluation and therefore included in the TOE is as follows:

- EnCase Enterprise Version 6.8 Admin Manual
- EnCase Enterprise Version 6.8 User Manual
- EnCase Enterprise Version 6.8 User Documentation Errata Sheet.

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for EnCase® Enterprise V6.8.

Evaluation team testing was conducted at the vendor's development site June 9 through June 12, 2008.

7.1 Developer Testing

Guidance Software's approach to testing for EnCase Enterprise is based on TOE Security Function (TSF) interface testing. Guidance has developed a test suite comprising various manual tests to exercise the TSF at the user interfaces as described in the TOE Functional Specification. The vendor addressed test depth by analyzing the functionalities addressed in the high-level design and associating test cases that cover the addressed functionalities. The high-level design addressed the general functions of the TOE subsystems, identifying the security functionality of each subsystem, as appropriate. The testing documentation maps security functions to specific test suites and tests, while the development documentation maps security functions to subsystems. The combination of the two mappings shows how the tests map to the subsystems.

The vendor ran the TOE test suites in various configurations, consistent with the test environment described in the testing documentation, and provided the evaluation team with the actual results. The test configurations were representative of the operating systems supported and the application environment. All tests passed.

7.2 Evaluation Team Independent Testing

The evaluation team executed the vendor test suite for EnCase Enterprise per the evaluated configuration as described in the Quality Assurance Test Plan.

The developer's test documentation identifies the tested configuration as EnCase Enterprise V6.8, comprising the SAFE, Examiner, and Servlet components.

The evaluation team conducted testing on Microsoft Windows Server 2003 SP1 environments, consistent with the environments specified in the ST.

The evaluation team devised a test subset based on coverage of the security functions described in the ST. The test environment described above was used with team generated test procedures and team analysis to determine the expected results.

The evaluation team performed the following additional functional tests:

- **Audit Record Generation**—this test sought to confirm that all of the auditable events identified in the ST (FAU_GEN.1) are actually audited. The result showed that the TSF does not audit "connecting to a role" or "disconnecting from a role".
- **Audit Record Deletion—user deletion**—confirm that user deletion events are audited. The test demonstrated that the TSF generates audit records for the user deletion events identified in the ST.
- **Minimum password length**—as reported in the AVA ETR, the vendor's SOF analysis bases its calculations partly on the claim that passwords have a minimum length of 6 characters with password construction requirements. However, none of these requirements, or any discussion of them, is included in the ST or user documentation. The user guidance documentation and functional specification indicate only that a password must meet certain construction requirements. This test identified conditions for different types of password.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product that searched a number of the sites considered by the developer. The developer's vulnerability search was comprehensive, and the evaluator's search was sufficient to validate the results provided by the developer. The evaluation team did not discover any new open source vulnerabilities/bugs that pertain to the TOE that have not been corrected. The evaluation team conducted the following additional penetration test for the reasons specified:

- **Examiner Capability on Local Machine (Identification and Authentication)**—The Examiner can be used to investigate the local machine without requiring user identification or authentication. The purpose of this test was to determine whether: a) this is possible without the Dongle being present; b) this is possible if the user does not have admin privileges on the local machine. The test demonstrated: a) the Dongle is required in order to exercise many of the Examiner capabilities on the local machine; b) the Examiner capabilities cannot be usefully exercised on the local machine if the user does not have administrative privileges on the local machine.

8 Evaluated Configuration

The evaluated version of the TOE is EnCase® Enterprise V6.8.

EnCase Enterprise is designed for corporate and government organizations that need the ability to perform internal computer investigations of all types. It establishes an investigative infrastructure that provides network-enabled search, identification, preservation, analysis and reporting of digital evidence on employee computers and file servers for the purposes of internal investigations such as fraud, HR matters and computer incident analysis and response. The solution views data at the binary level, providing the capability to find hidden files such as rootkits and identify zero-day exploits. In addition the software provides the ability to remediate malicious processes, and serves as a platform for add-on data discovery capabilities (not included in the evaluated configuration) for the purposes of sensitive data auditing and eDiscovery.

9 Results of the Evaluation

The evaluation was conducted based upon version 2.3 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each 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 validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an EAL2 certificate rating be issued for Guidance Software EnCase® Enterprise V6.8.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table:

TOE Security Assurance Requirements

Assurance Component ID	**Assurance Component Name**
ACM_CAP.2	CM Documentation
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Functional specification
ADV_HLD.1	High-level design
ADV_RCR.1	Representation Correspondence
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Test Coverage Analysis
ATE_FUN.1	Test Documentation
ATE_IND.2	Independent testing
AVA_SOF.1	Strength of TOE Analysis
AVA_VLA.1	Vulnerability analysis

10 Validator Comments/Recommendations

The user guidance for EnCase Enterprise includes documentation on several features of EnCase® Forensic that are not considered to be part of the evaluated configuration. The TOE security functions provide protection from data being downloaded from a system hosting a servlet, but this protection does not extend to the forensic data once it has been delivered to the Examiner component. Once the data has been exported to the Examiner as evidence files, those files are no longer under TSF control, allowing anyone with access to the Examiner workstation to manipulate the evidence files. Users are cautioned that the environment should be structured to restrict access to this information.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is **Guidance Software EnCase® Enterprise,** Version 1.0, dated 19 November 2008.

13 Bibliography

URLs

- NIAP Common Criteria Evaluation and Validation Scheme (http://www.niap-ccevs.org/cc-scheme/)
- SAIC CCTL (http://www.saic.com/infosec/common-criteria/)
- Guidance Software, Inc. (http://www.guidancesoftware.com)

NIAP CCEVS Documents:

- *Common Criteria for Information Technology Security Evaluatio*n, version 2.3, August 2005
- *Common Evaluation Methodology for Information Technology Security*, version 2.3, August 2005.

Other Documents:

- *Guidance Software EnCase® Enterprise Security Target*, Version 1.0, 19 November 2008.