National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Xceedium Gatekeeper
Version 4.0.0

Report Number: CCEVS-VR-07-0021

Dated: 9 May 2007
Version: 1.1

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

**Tim Bergendahl,
Paul Bicknell
The MITRE Corporation
Bedford, Massachusetts**

Common Criteria Testing Laboratory

**SAIC, Inc.
Columbia, Maryland**

Table of Contents

List of Tables

1 Executive Summary

The evaluation of **Xceedium GateKeeper Version 4.0.0** was performed by SAIC, in the United States and was completed in February 2007. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Xceedium TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3 and International Interpretations effective on 12, January 2007. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 1.0.

Science Applications International Corporation (SAIC) determined that the evaluation assurance level (EAL) for the product is EAL 3 family of assurance requirements. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Xceedium GateKeeper Version 4.0.0 Security Target.

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 GateKeeper product by any agency of the US Government and no warranty of the product is either expressed or implied.

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 validation team notes that the claims made and successfully evaluated for the product represent a more limited set of requirements than what might be used for a "normal" product deployment. Specifically, no claims are made for protection of data transmission between the TOE and non –TOE components such as the web browser and the network devices in spite of the fact that it will mostly likely be configured and setup in a distributed fashion over a network whose traffic could well be less than benign. It then becomes quite necessary for the administrators to fulfill the requirements levied on the environment.

The technical information included in this report was obtained from the Evaluation Technical Report for Xceedium GateKeeper Version 4.0.0 (ETR) Parts 1 and 2 produced by SAIC.

1.1 Evaluation Details

Evaluated Product: GateKeeper Version 4.0.0

Sponsor & Developer:
Xceedium, Inc.
30 Montgomery St., Suite 1020
Jersey City, NJ 07302

CCTL:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Completion Date: February 2007

CC: **Common Criteria for Information Technology Security Evaluation, Version 2.3**

Interpretations: There were no applicable interpretations used for this evaluation.

CEM: Common Methodology for Information Technology Security Evaluation, Version 1.0

Evaluation Class: EAL 3

Description

The TOE is a rack mounted secure access control appliance. The TOE provides remote IT support and monitoring to remote sites or local office locations via a Java enabled web browser. Common environments for use are datacenter branches and hosting/co-location facilities where network access methods, monitoring, and security are essential.

Users and administrators access the TOE, but only administrators can access and set TOE security functions. Administrators may perform the following TOE tasks: view logins, user sessions, and reporting; set configuration parameters and conduct maintenance tasks; create custom access; utilize management features; and set associations between users and devices. All administrative actions are mediated by an access control policy.

Disclaimer

The information contained in this Validation Report is not an endorsement of the Gatekeeper product by any agency of the U.S. Government and no warranty of the Gatekeeper product is either expressed or implied.

PP: none

Evaluation Personnel

Shukrat Abbas.
Craig Floyd

Validation Team: Tim Bergendahl,
Paul Bicknell
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730-1420

1.2 Interpretations

The evaluation team determined that there were no NIAP Interpretations applicable to this evaluation:

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

Table 1 - Threats

T.AUDIT_COMPROMISE	Unauthorized process or user	Illegal access to audit data
T.PRIVIL	Unauthorized user	Illegal access through the administrator interface
T.TSF_COMPROMISE	Unauthorized user or process	Illegal access to the TOE and its data
T.UNAUTH_ACCESS	Unauthorized user	Illegal access the network devices

2 Identification

The product being evaluated is GateKeeper Version 4.0.0. Note that the actual target of evaluation is defined to be only certain parts of the whole product.

3 Security Policy

Table 2 - Policies

P.MANAGE	The system must provide authorized administrators with utilities to effectively manage the security functions of the TOE
P.PROTECT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.
P.AUDIT	Users of the system shall be held accountable for their security relevant actions within the system.

4 Assumptions

4.1 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

Table 3 – Personnel Assumptions

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4.2 Physical Assumptions

The following physical assumptions are identified in the Security Target:

Table 4 – Physical Assumptions

A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

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. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made; and meets them with only a certain level of assurance (EAL 3 in this case).
2. As with all EAL 3 evaluations, this evaluation did not specifically search for vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM); or seriously attempt to find counters to them; nor find vulnerabilities related to objectives not claimed in the ST.
3. Encryption of communications using SSL between the web browser and the TOE and between the TOE and network devices is mentioned in some of the evaluation documents yet no requirements for it are included in the ST. Furthermore there are no requirements for any protection of data sent between the appliance and the web browser and the appliance and network devices. However, the evaluation team did verify the SSL communication between the browser and the TOE and the TOE and the back-end devices. Testing confirmed the presence of encrypted communication.
4. Note also that certain features of the product are not evaluated:
   a. Fail Over Capability
   b. Use of a Radius Server

c. Whole Security Scan
d. Use of a Modem
e. SNMP
f. NTP communication
g. Active Directory Server

5 Architectural Information

The TOE is a rack mounted secure access control appliance. The TOE provides remote IT support and monitoring to remote sites or local office locations via a Java enabled web browser. Common environments for use are datacenter branches and hosting/co-location facilities where network access methods, monitoring, and security are essential.

An administrator configures TOE user access to network devices. The administrator configures custom module permissions per user to the specific network devices. User entity includes both account and contact information. Both an administrator and a user can update the user's account information for username, password, first name, last name, phone number, beeper number, email address, and other description such as department, location, etc.

Users and administrators access the TOE, but only administrators can access and set TOE security functions. Administrators may view logins, user sessions, and reporting; set TOE configuration parameters; and conduct maintenance tasks; create custom access; utilize management features; and set associations between users and devices. All administrative actions are mediated by an access control policy.

The TOE implements the following evaluated features:

1. External appliance LCD display for entering initial host connection information or checking on system configuration.
2. Authentication via TOE web server
3. Single Access Port to network devices
4. Web interface GUI for administrators and users
5. Monitoring, logging, and alert emails for monitored events

This product is meant to be used in an environment where the support personnel are not local to the back-end devices and access is restricted via other means such as firewalls. In that scenario, only legitimate users with valid authentication credentials will be able to access services that were defined for them.

6 Documentation

Following is a list of documents supplied by the developer on a CD shipped with the product.

- Xceedium GateKeeper v4.0.0 Administration Guide v4.1, February 2007

- Xceedium GateKeeper v4.0.0 Installation Guide, v4.2, February 23, 2007
- Xceedium GateKeeper v4.0.0 User's Guide, v4.1, February 2007
- README file – contains an overall description of CD contents and basic system requirements

The security target used is:

- Xceedium GateKeeper Version 4.0.0 Security Target, version 2.0, April 4, 2007.

7 IT Product Testing

The evaluation team applied each EAL 3 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST. The tests were conducted using:

- TOE Server Platform: GateKeeper v4.0.0 appliance
- TOE Client Platform: Windows XP SP2 and Java-enabled web browser
- Network Devices: Sun OS, Windows 2003 server, Windows NT, Linux OS, Cisco router, net KVM, Power management devices

The basic test configuration is an administrator or user running a Java-enabled Web browser on a client machine performing functions on the TOE appliance. The following tasks were performed by the evaluation team:

The developer test suite was examined and found to provide adequate coverage of the security functions.

A selection of the developer tests were run and the results found to be consistent with the results generated by the developer.

Tests devised from postulated vulnerabilities in the I&A mechanism revealed no problems.

In addition, no vulnerabilities in the TOE were found during a search of vulnerability databases.

8 Evaluated Configuration

The evaluated configuration is a single Gatekeeper being accessed over a network from a single Web browser.

9 Results of the Evaluation

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The validation team observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validation team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR.

The validation team, therefore, recommends that the evaluation and Pass result for the identified TOE be accepted.

11 Annexes

Not applicable.

12 Security Target

The security target for this product's evaluation is **Xceedium GateKeeper Version 4.0.0 Security Target**, Version 2.0, April 4, 2007.

13 Glossary

There were no definitions used other than those used in the CC or CEM.

Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 2005, version 2.3.

[7] Evaluation Technical Report for Xceedium GateKeeper Version 4.0 Part II, version 2.0, April 5, 2007

[8] Xceedium GateKeeper Version 4.0 Security Target, Version 2.0, April 4, 2007.

[9] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001