National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

ATEN/IOGear Secure KVM Switch Series

Report Number: **CCEVS-VR-10446-2011**
Dated: **July 1, 2011**
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

<u>Validation Team</u>

<u>Common Criteria Testing Laboratory</u>

Table of Contents

List of Tables

1   Executive Summary

The evaluation of **ATEN/IOGear Secure KVM Switch Series** was performed by SAIC, in the United States and was completed in June 2011. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the ATEN/IOGear Secure KVM Switch Series TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 3. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation versions 3.1, revision 3.

Science Applications International Corporation (SAIC) determined that the product satisfies evaluation assurance level (EAL) 2 augmented with ALC_FLR.2 as defined within the Common Criteria (CC). The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the ATEN/IOGear Secure KVM Switch Series Security Target, Version 1.5, 2 June 2011.

This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is a collection of hardware devices as follows:

ATEN Secure KVM Model CS1182

ATEN Secure KVM Model CS1184

IOGear Secure KVM Model GCS1212TAA

IOGear Secure KVM Model GCS1214TAA

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) 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 ATEN/IOGear Secure KVM Switch Series 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 evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and versions of the ETR. Also, at some discrete points during the evaluation, validators formed a Validation Oversight Review panel in order to review the Security Target and other evaluation evidence materials along with the corresponding evaluation findings in detail. The validation team found that the evaluation showed that the product satisfies all of the security functional 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 technical information included in this report was obtained from the Final Evaluation Technical Report for the ATEN/IOGear Secure KVM Switch Series Parts I and II and the associated test report produced by SAIC.

1.1 Evaluation Details

Evaluated Product: ATEN/IOGear Secure KVM Switch Series

ATEN Secure KVM Model CS1182

ATEN Secure KVM Model CS1184

IOGear Secure KVM Model GCS1212TAA

IOGear Secure KVM Model GCS1214TAA

Sponsor & Developer: ATEN/IOGear

CCTL: Science Applications International Corporation
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, MD 21046

Completion Date: June 2011

CC: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009

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

CEM: Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 3, July 2009

PP: Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 2.1, September 07, 2010

Evaluation Class: Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2

Description   The ATEN/IOGear Secure KVM Switch Series products are peripheral port sharing switches, known as KVMs, that facilitate the secure switching of a common set of user input/output devices among attached computers.

Disclaimer   The information contained in this Validation Report is not an endorsement of the ATEN/IOGear Secure KVM Switch Series products by any agency of the U.S. Government and no warranty of ATEN/IOGear Secure KVM Switch Serie is either expressed or implied.

Evaluation Personnel: James Arnold

Julie Cowan

Quang Trinh

Validation Team: Jean Petty

                                          W. Olin Sibert

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation. Note that assurance requirements outside the scope of EAL 1 through EAL 4 are addressed at the discretion of the CCEVS.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

The following table serves to identify the evaluated Security Target and TOE.

Table 1 ST and TOE identification

ST Title:	ATEN/IOGear Secure KVM Switch Series Security Target, Version 1.5.1, 28 June 2011
TOE Identification:	ATEN/IOGear Secure KVM Switch Series ATEN Secure KVM Model CS1182 ATEN Secure KVM Model CS1184 IOGear Secure KVM Model GCS1212TAA IOGear Secure KVM Model GCS1214TAA
Operating Environment:	Console USB keyboard USB mouse DVI-I monitor Audio Input/Output devices (e.g., Microphone and Speakers) Computer Workstations/Servers with USB connection (for keyboard and mouse) DVI-I connection Audio Input/Output connections

3 Threats to Security

The following are the threats that the evaluated product addresses:

3.1 TOE Threats

T.INVALIDUSB - The AUTHORIZED USER will connect unauthorized USB devices to the peripheral switch.

T.RESIDUAL - RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs.

T.ROM_PROG - The TSF may be modified by an attacker such that code embedded in reprogrammable ROMs is overwritten, thus leading to a compromise of the separation-enforcing components of the code and subsequent compromise of the data flowing through the TOE.

T.SPOOF - Via intentional or unintentional actions, a USER may think the set of SHARED PERIPHERALS are CONNECTED to one COMPUTER when in fact they are connected to a different one.

T.TRANSFER - A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.

4   Assumptions

The following assumptions are identified in the Security Target:

4.1   Physical Assumptions

The following physical assumptions are identified in the Security Target.

A.PHYSICAL - The TOE is physically secure.

4.2   Personnel Assumptions

The following personnel assumptions are identified in the Security Target.

A.ACCESS - An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.

4.3   Intended Use Assumptions

The following intended use assumptions are identified in the Security Target.

A.NOEVIL - The AUTHORIZED USER is non-hostile and follows all usage guidance.

A.MANAGE - The TOE is installed and managed in accordance with the manufacturer's directions.

Application Note: It is further assumed that the installed USB devices connected to the TOE do not buffer and transfer data to other COMPUTERS except the currently CONNECTED COMPUTER.

5 Architectural Information

The TOE combines KVM (USB Keyboard, DVI-I Video, USB Mouse) switch functionality (2/4 port KVM switch) and audio (input & output) ports.

The TOE is normally installed in settings where a single USER with limited work surface space needs to access two or more COMPUTERS, collectively termed SWITCHED COMPUTERS (which need not be physically distinct entities). The USER may have a KEYBOARD, a visual display (e.g., MONITOR), a POINTING DEVICE (e.g., mouse) and audio input/output device. These are collectively referred to as the SHARED PERIPHERALS.

In operation, the TOE will be CONNECTED to only one COMPUTER at a time. To use a different COMPUTER, the USER must perform some specific action. The TOE will then visually indicate which COMPUTER was selected by the USER. Such indication is persistent and not transitory in nature.

The architecture of the TOE is quite simple. It is a physical device with two USB (one for a mouse and one for a keyboard), one DVI, and two audio connections for the user accessible keyboard, mouse, monitor, and audio (e.g., speakers and microphone) devices and also two or four (depending on the specific device) sets of connections for two or four attached computers. These connections to attached computers consist of one USB, one DVI, and two audio connections. The device has a power switch and two or four buttons corresponding to the attachable computers. When the user selects a given computer with a button, the appropriate connections are made (and a LED indicator identifies the currently switched computer).

Internally, the audio and DVI connections are established using analog relays and other than making the appropriate connections the TOE does not process the signals passing across the connections. On the other hand, the TOE interprets the signals of the attached key board and mouse, allowing only inputs from the devices and sending only keyboard cap lock, scroll lock, and num lock signals to the keyboard. Internally, it emulates a keyboard and mouse connected to each attached computer and brokers the keyboard and mouse signals for the current connection.

5.1 Physical Boundaries

The TOE is a hardware product, and as such the physical boundary of the TOE is simply the device and its associated ports, power switch, selector buttons, and LED indicators. The specific TOE models are as follows:

- ATEN Secure KVM Model CS1182
- ATEN Secure KVM Model CS1184
- IOGear Secure KVM Model GCS1212TAA
- IOGear Secure KVM Model GCS1214TAA

The TOE attaches to other devices as follows:

- Console

- o USB keyboard
- o USB mouse
- o DVI-I monitor
- o Audio Input/Output devices (e.g., Microphone and Speakers)

- Computer Workstations/Servers with:
  - o USB connection (for keyboard and mouse)
  - o DVI-I connection
  - o Audio Input/Output connections

6 Documentation

Following is a summary of user documents supplied by the developer for the TOE:

- USB DVI Secure KVM Switch CS1182 / CS1184 User Manual v1.2

- USB DVI Secure KVM Switch GCS1212TAA / GCS1214TAA User Manual v1.2

The security target used is:

- ATEN/IOGear Secure KVM Switch Series Security Target, Version 1.5, 2011/06/02

7 IT Product Testing

The purpose of this activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST for an EAL2+ evaluation.

7.1 Developer Testing

The developer created test procedures specifically to fulfill the test requirements for an EAL2+ evaluation. The tests were developed to provide good coverage of the security functions related to each of the security requirements in the Security Target. The developer has documented their tests in a test plan where the results of the tests are presented as prose conclusions, notes, screen shots, and summaries for each of the applicable test platforms.

7.2 Independent Testing

Independent testing took place in essentially two phases.

The evaluators received the TOE in the same manner as normal customers, installed and configured the TOE in accordance with the provided guidance, and exercised a subset of the developers test plan on equipment configured in the testing laboratory. This effort involved installing and configuring all four of the KVM models identified in the ST. Subsequently, the evaluators exercised a subset of the available developer's test procedures for all of the evaluated KVM models. With the exception of the tamper tests, all of the developer tests were exercised successfully on all of the KVM models. The tamper tests were exercised on only one device and the results were extrapolated to cover the other models as deemed appropriate.

Also, the evaluators devised independent tests to ensure that power-off/on conditions were addressed, that there were no inadvertent means of transmitting data among attached computers, and to ensure that a broader set of USB devices resulted in not being usable (only keyboards and mice are supposed to work).

In addition to the use of developer provided and independently devised security functional tests, the evaluators also explored possibilities to penetrate or bypass the security mechanisms. Much of this work was based on analysis of the design and actual use of the products. Applicable tests included attempts to identify audio cross talk among computer and attach device audio connections and also to further investigate the tamper detection capabilities.

Given the complete set of test results from test procedures exercised by the developer and the sample of tests directly exercised by the evaluators, the testing requirements for EAL2+ are fulfill.

8 Evaluated Configuration

The TOE is one of the identified ATEN/IOGear Secure KVM Switch Series products attached to suitable devices as summarized above and in the ST.

9 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC, the CEM, and the CCEVS. The validation team found that the evaluation showed that the product satisfies all of the

security functional and assurance requirements stated in the Security Target (ST). The validation team concluded that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. Additional validator comments are included in section 10, below.

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 the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing notes, comments, or vendor actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. 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. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part I, states:

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary part of the ETR (see Chapter 15).

> 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 CC version 3.1 [1], [2], [3] and CEM version 3.1 [4]. The evaluation determined the TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 2) requirements, augmented with ALC_FLR.2. The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report for the ATEN/IOGear Secure KVM Switch Series Part 2" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> *Section 6.1, ST Evaluation:* "Each verdict for each CEM work unit in the ASE ETR is a 'PASS'. Therefore, the ST is a CC compliant ST."

> *Section 6.2, TOE Evaluation:* "The verdicts for each CEM work unit in the ETR sections included in the proprietary part of the ETR (see Chapter 15) are each 'PASS'. Therefore, the TOE (see below product identification) satisfies the Security Target, when configured according to the following guidance documentation:

USB DVI Secure KVM Switch CS1182 / CS1184 User Manual v1.2

USB DVI Secure KVM Switch GCS1212TAA / GCS1214TAA User Manual v1.2

Additionally, the evaluation team's performance of developer tests, independent tests, and penetration tests further demonstrates the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The following should be considered by potential users of the TOE:

1. The TOE claims tamper-related capabilities, including tamper stickers and a tamper switch attached to the device chassis; however the validators found that these features may have limited effectiveness in a hostile environment. The user should note assumptions included

in the ST and consider these carefully. These include an assumption that the TOE operating environment is physically secure, that the user is non-hostile and follows all usage guidance, and that the TOE is installed and operated according to all manufacturer instructions.

2. The user is cautioned that the TOE includes a tamper-related deactivation function that, when triggered, requires return of the device to the developer for reactivation. The user must ensure that this type of return and reactivation is consistent with the security requirements for service and maintenance in the user's specific environment.

11 **Annexes**

Not applicable.

12 **Security Target**

ATEN/IOGear Secure KVM Switch Series Security Target, Version 1.5, 2011/06/02

13 Acronym List

CC	Common Criteria
CCTL	CC Testing Laboratory
CI	Configuration Item
CM	Configuration Management
DoD	Department of Defense
DVI-I	Digital Video Interface - Integrated
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FSP	Functional Specification
IT	Information Technology
KVM	Keyboard-Video-Mouse
LED	Light Emitting Diode
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
PP	Protection Profile
SAIC	Science Applications International Corporation
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
USB	Universal Serial Bus

14 **Bibliography**

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

[1]   Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 3, July 2009.

[2]   Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 3, July 2009.

[3]   Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009.

[4]   Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009.

[5]   ATEN/IOGear Secure KVM Switch Series Security Target, Version 1.5, 2 June 2011.

[6]   Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7]   SAIC CCTL Evaluation Procedures Annex, Version .20, January 31 2004.