Swedish Certification Body for IT Security

Certification Report - HSL KVM Combiner

Issue: 1.0, 2020-Aug-27

Authorisation: Jerry Johansson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is a keyboard, mouse and video switch, consisting of one of the hardware appliances:

TC82PHG-3T 8:2 Secure Combiner,

TC82PHG-3T 8:2 Secure Combiner Gen II,

TC162PHG-3T 16:2 Secure Combiner,

TC162PHG-3T 16:2 Secure Combiner Gen II,

with firmware: 44403-E7E7.

The major security feature is prevention of data leakage between different computer ports.

The TOE is delivered to the user as a single package ready for use, with all necessary cabling, and via a trusted courier. Guidance is available on-line.

No Protection Profiles are claimed.

There are four assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the five threats in the ST. The assumptions, the threat and the OSP are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by Combitech AB and EWA-Canada Ltd. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation was performed at the evaluation assurance level EAL 4, augmented by ALC_FLR.3 Systematic flaw remediation.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation. EWA-Canada Ltd. operates as a Foreign location for Combitech AB within scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 4 + ALC_FLR.3

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by Combitech AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.
This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2019008
Name and version of the certified IT product	HSL KVM Combiner consisting of one of the hardware appliances: TC82PHG-3T 8:2 Secure Combiner, TC82PHG-3T 8:2 Secure Combiner Gen II, TC162PHG-3T 16:2 Secure Combiner, TC162PHG-3T 16:2 Secure Combiner Gen II, with firmware: 44403-E7E7
Security Target Identification	HSL Secure KVM Combiner Switches Security Target, High Sec Labs Ltd., 2019-09-20, document version 1.0.
EAL	EAL 4 + ALC_FLR.3
Sponsor	High Sec Labs Ltd.
Developer	High Sec Labs Ltd.
ITSEF	Combitech AB and EWA-Canada Ltd.
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.23.2
Scheme Notes Release	15.0
Recognition Scope	CCRA and SOGIS
Certification date	2020-08-27

3 Security Policy

The TOE provides the following security fetures:

- Video security
- Keyboard and Mouse security
- Hardware Anti.Tampering Indication

3.1 Video Security

• Computer video input interfaces are isolated through the use of different electronic components, power and ground domains
• The display is isolated by a dedicated, read-only, Extended Display Identification Data (EDID) emulation for each computer
• Access to the monitor's EDID is blocked
• Access to the Monitor Control Command Set (MCCS commands) is blocked

3.2 Keyboard and Mouse Security

• The keyboard and mouse are isolated by dedicated, Universal Serial Bus (USB) device emulation for each computer
• One-way, peripheral-to-computer data flow is enforced through unidirectional optical data diodes
• Communication from computer-to-keyboard/mouse is blocked
• Non HID (Human Interface Device) data transactions are blocked

3.3 Hardware Anti-Tampering Indication

• Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes four assumptions on the usageand operational environment of the TOE:

A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data that passes through the TOE, is assumed to be provided by the environment.

A.TRUSTED_CONFIG

Personnel installing and configuring the TOE and its operational environment will follow the applicable guidance.

A.TRUSTED_USER

TOE users are trusted to follow and apply all guidance and security procedures in a reliable manner.

A.USER_IDENT

The operational environment is responsible for the identification and authentication of users. This determines physical access to the TOE, and access to the connected computers and their applications and resources.

4.2 Clarification of Scope

The Security Target contains five threats, which have been considered during the evaluation:

T.DATA_LEAK

An unauthorized user may be able to access data that is transmitted via an unauthorized data transfer through the TOE or its connected peripherals.

T.PHYSICAL_TAMPER

A malicious user could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.

T.SWITCHING

A poorly designed TOE could result in a situation where a user is connected to a computer other than the one to which the user intended to connect, resulting in an unintended flow of data.

T.UNAUTH

A malicious user could tamper with the security attributes that determine allowed peripheral devices and allowed data flows, resulting in the use of unauthorized peripheral devices that may allow unauthorized data flows between connected devices, or an attack on the TOE or its connected computers.

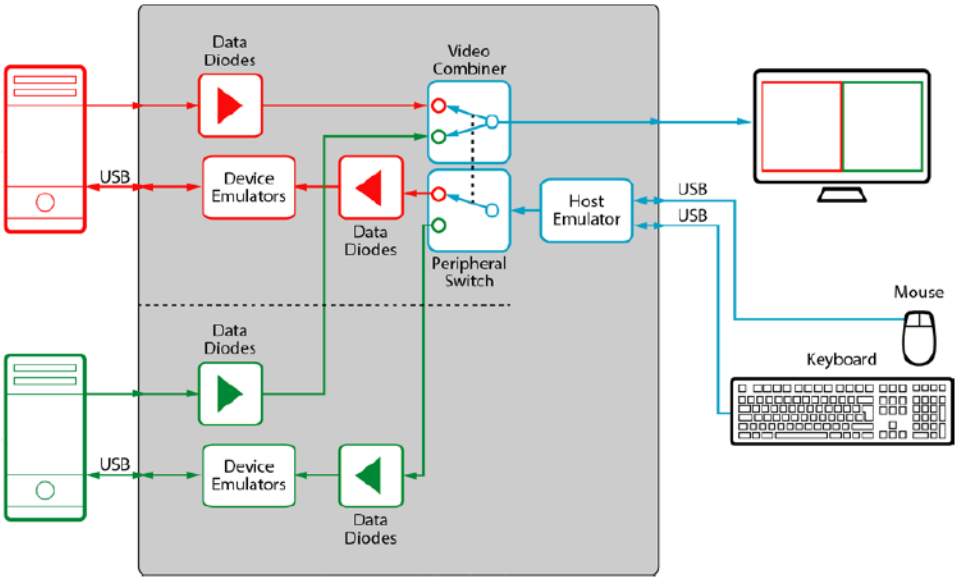
T.UNAUTH_DEVICE

A malicious user could connect an unauthorized peripheral device to the TOE, and that device could cause information to flow between connected devices in an unauthorized manner, or could enable an attack on the TOE or its connected computers.

The Security Target does not contain any Organisational Security Policy (OSP).

5 Architectural Information

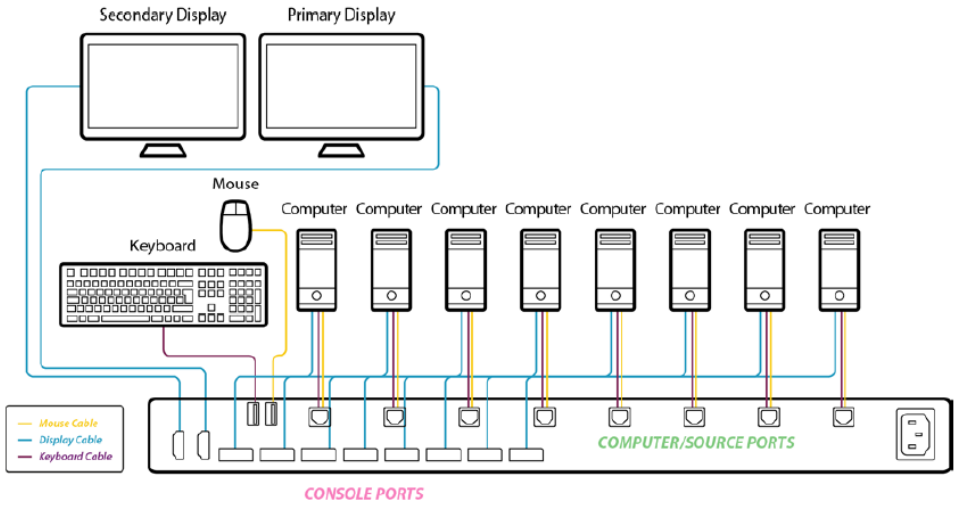
In the figure below, the TOE is shown with grey background.



The Video Combiner combines and presents the video input on the console monitors.

The peripheral switch multiplexer ensures the selection of just one keyboard / mouse serial data source at any given time.

In the evaluated configuration, the TOE has two displays and can connect up to eight (shown below) or up to sixteen computers, depending on the hardware appliance.



6 Documentation

The following documents are included in the scope of TOE:

High Sec Labs Secure 8/16 Port Combiner User Manual, High Sec Labs Ltd., document number 18240, revision 1.0

HSL Secure KVM Combiner Switches Common Criteria Guidance Supplement, High Sec Labs Ltd. 2019-08-02, document version 1.0

7 IT Product Testing

7.1 Developer Testing

The developer tested the TSF with full coverage and depth for all four models of the TOE. The developer testing was done between 2019-08-18 and 2019-08-21 in the developer's premises in Caesarea, Israel.

7.2 Evaluator Testing

The evaluators repeated almost all developer test cases. Some of the test cases were run with all four TOE models, some on three, two, or one model. The evaluators also devised a few independent test cases, which were tested with two TOE models.

Most of the evaluator testing was performed between 2019-08-18 and 2019-08-22 in the developer's premises in Caesarea, Israel. Some additional tests were performed in the evaluator's premises in Växjö, Sweden in January 2020.

7.3 Penetration Testing

The penetration testing was done with one TOE model. The evaluators devised one penetration test case. The testing took place in the evaluator's premises in Växjö, Sweden in January 2020.

8 Evaluated Configuration

Wireless keyboards and mice are not allowed in the evaluated configuration.

During the tests, Windows 7, Windows 8.1, Windows 10, and Windows Server 2008 R2, host machines were connected to the TOE's ports. However, the use of other operating systems is supported, and does not affect the security functionality of the TOE.

Touch screens were not used during the tests. Touch screens function as ordinary screens, i.e. without touch functionality, when used with the TOE.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Enhanced-Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.4	PASS
TOE Design	ADV_TDS.3	PASS
Implementation Representation	ADV_IMP.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.4	PASS
CM Scope	ALC_CMS.4	PASS
Delivery	ALC_DEL.1	PASS
Development Security	ALC_DVS.1	PASS
Life-cycle Definition	ALC_LCD.1	PASS
Flaw Remediation	ALC_FLR.3	PASS
Tools and Techniques	ALC_TAT.1	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.2	PASS
Depth	ATE_DPT.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.3	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

EDID	Extended Display Identification Data
EEPROM	Electrically Erasable Programmable Read-Only Memory
HDMI	High-Definition Multimedia Interface
HID	Human Interface Device
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
KVM	Keyboard, Video, Mouse
MCCS	Monitor Control Command Set
ST	Security Target
TOE	Target of Evaluation
UHD	Ultra-High Definition
USB	Universal Serial Bus

12 Bibliography

ST	HSL Secure KVM Combiner Switches Firmware 44403-E7E7 Security Target, High Sec Labs Ltd., 2020-07-17, document version 1.1, 19FMV3575-25
Man	High Sec Labs Secure 8/16 Port Combiner User Manual, High Sec Labs Ltd. 2019-08-02, document number 18240, revision 1.0, 19FMV3575-11
Supp	HSL Secure KVM Combiner Switches Common Criteria Guidance Supplement, High Sec Labs Ltd. 2019-08-02, document version 1.0, 19FMV3575-11
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1, revision 5, April 2017, CCMB-2017-04-003
CC	CCpart1 + CCPart2 + CCPart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, April 2017, CCMB-2017-04-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2019-09-24, document version 31.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
1.23.2	2020-05-11	None
1.23.1	2020-03-06	None
1.23	2019-10-14	None
1.22.3	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	3.0	Demonstration of test coverage	Clarify test coverage of the TSFI
SN-18	1.0	Highlighted Requirements on the Security Target	Clarifications on the content of the ST
SN-22	2.0	Vulnerability Assessment	Clarifications regarding vulnerability assessment