Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australasian Information Security Evaluation Program

Certification Report

PacketLight PL-2000 Series with Firmware v1.3.12c

Version 1.0, 18 September 2020

cyber.gov.au

ACSC Australian Cyber Security Centre

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of PacketLight PL-2000 Series with Firmware v1.3.12c against Common Criteria EAL2+ALC_FLR.1.

The Target of Evaluation (TOE) is PacketLight PL-2000 Series with Firmware version 1.3.12c. The TOE is an optical transport network (OTN) device with layer 1 encryption capabilities. Layer 1 encryption can be an important part of a multiple-layer encryption strategy where encryption of bulk data transport at layer 1 protects higher layer data transfer.

The PL-2000AD, PL-2000M and the PL-2000ADS are three product variations from the PL-2000 series base. The product variants run the same firmware and provide the same security functions and mechanisms with minor changes in the network ports. The devices provide a Multi-Service Provisioning Platform (MSPP) in 1U of rack space. The PL-2000AD is a long-haul device, the PL-2000M is for metropolitan networks and the PL-2000ADS is for short-haul applications. Data services fed into the TOE can be simply encapsulated, aggregated or multiplexed to or from the TOE transport link(s). Data services communicated between multiple connected instances of the TOE can be encrypted at layer 1 to ensure secure communication between devices. Encryption can be over the entire transport link or alternatively managed per service.

This report concludes that the TOE has complied with the Common Criteria (CC) evaluation assurance level EAL2 augmented with ALC_FLR.1 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP).

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program. The evaluation was performed by Teron Labs and was completed on 31 August 2020.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that:

- users review their operational environment and ensure security objectives for the operational environment can be met
- users configure and operate the TOE according to the vendor's supplementary guidance
- users make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- users and managers of the TOE understand the strict security model provided by the TOE when multiple Crypto Officers share the cryptographic functionality of the TOE on a per service basis.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target [7] and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [7] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is PacketLight PL-2000 Series with Firmware v1.3.12c.

Description	Version
Evaluation scheme	Australasian Information Security Evaluation Program
TOE	PacketLight PL-2000 series models PL-2000AD, PL-2000ADS and PL-2000M
Firmware version	1.3.12c
Security Target	*PacketLight PL-2000 Series with Firmware v1.3.12c Version 1.3 dated 31 August 2020*
Evaluation Technical Report	*Evaluation Technical Report 1.0 dated 31 August 2020* Document reference EFT-T010-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Conformant and Part 3 Augmented Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	EAL 2 augmented with ALC_FLR.1
Developer	PacketLight Networks Ltd

	27 Habarzel St Tel-Aviv 6971039 Israel
Evaluation facility	Teron Labs Pty Ltd Unit 3, 10 Geils Court Deakin ACT 2600 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is PacketLight PL-2000 Series with Firmware 1.3.12c. The models considered are the PL-2000AD, PL-2000ADS and PL-2000M.

The TOE is intended to provide secure communications transport facilities over fibre-optic links. Each end of the fibre-optic transport link must use matching fibre-optic hardware and low level protocols. When licensed and enabled for encryption, each end of the transport link must also have matching cryptographic keys for the link to function correctly. The three evaluated models vary in the distance of fibre-optic transport link they can provide. The PL-2000AD is intended for long haul or metropolitan distance application. The PL-2000M is intended for metropolitan distance or short haul application. The PL-2000ADS is intended for short haul application.

The TOE can accept a single service or aggregate a number of lower bitrate services that are then carried over the transport links described above. The transport link protocol has been designed to carry a number of commonly used services such as LAN or storage network protocols. The TOE can be configured to encrypt the transport link as a whole or to manage the encryption of the services individually.

The TOE can be managed locally with a command line interface over a serial port, remotely with a command line interface over SSHv2 and with a graphical user interface over HTTPS. The TOE implements the cryptographic protocols to protect communications between itself and a remote management station.

Other security functionality provided by the TOE includes:

- the generation and storage of audit records
- user authentication and support of various security roles
- well defined management functions allowed by various security roles
- firewall function to exclude out-of-scope protocols.

The TOE provides physical and logical tamper evidence mechanisms. Tamper evident seals are used for physical protection. TOE users can execute self-test functions to ensure authenticity of the TOE firmware.

An optical signal power level measurement function can detect changes in the fibre-optic signals which might indicate a fault or possible tampering with the fibre-optic signal path.

TOE Functionality

The TOE functionality that was evaluated is described in section 2.4.2 of the Security Target [7].

TOE physical boundary

The TOE physical boundary is described in section 2.4.1 of the Security Target [7].

TOE Architecture

The TOE is intended to be operated as an element in carefully configured matching groups of TOE units. The simplest architecture being a matching pair of TOEs with matching port configurations. PacketLight should be consulted for information on the full range of configurations possible.

Inside the physical casing of the TOE there are subsystems providing power, cooling, optical functions, communications protocol functions, encryption functions and resources for system control. The system control function has been built using a typical layered approach. The TOE allows for the management of this control function via various means including a serial port that can be connected locally, a SSHv2 protected command line interface that can be used locally or remotely and a HTTPS protected graphical user interface that can be used locally or remotely.

Clarification of scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [7].

Non-evaluated functionality and services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Protocols not included in the scope of the evaluation include:

- Telnet
- Hypertext Transfer Protocol (HTTP)
- Simple Network Management Protocol Version 1 (SNMPv1)
- Simple Network Management Protocol Version 2 (SNMPv2)
- Simple Network Management Protocol Version 3 (SNMPv3)
- RADIUS for remote user authentication
- Rapid Spanning Tree Protocol (RSTP)
- Trivial File Transfer Protocol (TFTP)
- Secure or SSH File Transfer Protocol (SFTP)
- Simple Network Time Protocol (SNTP)
- Syslog Protocol
- Virtual chassis configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [4] for policy relating to using an evaluated product in an unevaluated configuration. New Zealand Government users should consult the *New Zealand Information Security Manual* [5].

Security

The TOE Security Policy is a set of rules that defines how information within the TOE is managed and protected. The Security Target [7] contains a summary of the evaluated functionality.

Usage

Evaluated configuration

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as described in the PacketLight PL-2000 Common Criteria Guidance Supplement v2.2.

Important aspects include:

- The Admin password must be changed
- The 21 Crypto Officer passwords must be changed
- Cryptography licences must be obtained and installed
- The firmware version must be 1.3.12c
- If the firmware version is any other than 1.3.12c the firmware must be updated in accordance with the guidance in [6]. The firmware file name must be pl_1_3_12c.tar with the following SHA-256 checksum: 9d 39 2b 9e 13 3a f8 88 fb e0 e5 d3 d0 8c 23 09 e9 87 61 43 58 60 5e f9 33 1b 35 a1 73 63 fe dc
- Management can only be undertaken via local serial connection command line interface, a SSHv2 accessed command line interface or a HTTPS accessed graphical user interface.

Secure delivery

Hardware and Licence delivery procedures

The product is delivered to customers in a standard package which PacketLight have developed to avoid shipping damage. The chassis is supplied with only the power supplies (dual, redundant, hot-swappable) and the fan unit pre-installed.

The recipient must verify that the TOE identification printed in the front panel corresponds to the version ordered (i.e. PL-2000AD, PL-2000M or PL-2000ADS).

All optics modules (uplink and client services) are included in a separate carton within the main package, to be plugged in by the customer once the chassis has been mounted in the rack. Customers typically nominate the client services they wish to run within the transport payload.

PacketLight supplies the optical modules (SFP+, QSFP) for this. Other optical modules from alternative suppliers are generally not interoperable with the PacketLight PL-2000 series and must not be used.

The recipient must verify that all components of the TOE are received and contact their distributor or reseller immediately if any component is missing. If that is the case, the TOE must not be used.

The encryption licence for each PL-2000 series unit is supplied by email post-delivery, by reference to the Chassis ID. This licence file is applied during the initial configuration of the TOE. If no encryption licence is applied, the TOE will operate but shall not be in a certified configuration and, therefore, must not be used in applications requiring Common Criteria certification.

The PacketLight PL-2000 Series Common Criteria Guidance Supplement [6] is downloaded by the customer with information provided by PacketLight. The TOE shall at all times be operated in accordance with this guidance.

Installation of the TOE

The installation procedure is contained in the guidance documentation [6]. The procedure is summarized as follows:

The TOE is shipped with the initial user account Admin (with a default password Admin) and 21 Crypto Officer accounts (each one has a default password specified in the model user manual [6]). The default passwords MUST be changed immediately by the administrator.

Cryptography licences are obtained by email and are associated to the Chassis ID of the TOE.

Upon the first boot-up of the TOE, the recipient shall also verify the firmware version number to ensure that it is 1.3.12c.

Version verification

The version of PacketLight PL-2000 series firmware being run can be verified from the General Tab in the System Configuration window of the graphical user interface for controlling the TOE. In the evaluated configuration this will be 1.3.12c.

Documentation and guidance

The general user documentation for PacketLight PL-2000 series with Firmware v1.3.12c and the Common Criteria Guidance Supplement included in the scope of the TOE are available on-line from the PacketLight product portal after purchase. The model and version specific user documents are [6]:

- PacketLight Networks PL-2000AD 1.3 User Manual
- PacketLight Networks PL-2000ADS 1.3 User Manual
- PacketLight Networks PL-2000M 1.3 User Manual.

The Common Criteria Guidance is in Packetlight PL-2000 Series Common Criteria Guidance Supplement Version 2.2, 31 August 2020 [6].

All Common Criteria material is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [4]. The *New Zealand Information Security Manual* is available at https://www.gcsb.govt.nz/ [5].

Secure usage

The evaluation of the TOE took into account certain policies specified for the operational environment. These policies must be enforced in order to ensure the security objectives of the TOE are met.

- The TOE administrators are trustworthy, trained and administer the TOE according to guidance
- The TOE and the management workstation used to control it reside in physically secure premises.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

Evaluation procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3* [1, 2].

Testing methodology was drawn from *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5* [3].

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program [10].

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* were also upheld [9].

Functional testing

To gain confidence that the developer testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining the test coverage, test plans and procedures, and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

These developer tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All Security Functional Requirements listed in the Security Target [7] were exercised during testing.

Penetration testing

A vulnerability analysis of the TOE was conducted in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

The evaluator performed a vulnerability analysis of the TOE in order to identify any obvious security vulnerability in the product, and if identified, to show that the security vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible security vulnerabilities in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

- time taken to identify and exploit (elapsed time)
- specialist technical expertise required (specialist expertise)
- knowledge of the TOE design and operation (knowledge of the TOE)
- window of opportunity
- IT hardware/software or other equipment required for the exploitation.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

EAL2 provides assurance by a full security target and an analysis of the Security Functional Requirements (SFRs) in that security target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE Security Functionality (TSF), evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

Certification result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [7] and **has met** the requirements of Common Criteria EAL2+ALC_FLR.1.

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [8], the Australasian Certification Authority **certifies** the evaluation of PacketLight PL-2000 Series with Firmware v1.3.12c performed by the Australasian Information Security Evaluation Facility, Teron Labs.

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual* [4] and New Zealand Government users should consult the *New Zealand Information Security Manual* [5].

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

In addition to ensuring that the stated Organizational Security Policies are applicable the Australasian Certification Authority also recommends:

- that the TOE is operated in the evaluated configuration
- users configure and operate the TOE in accordance with the vendor's supplementary guidance and pay attention to all security warnings

- users review their operational environment and ensure security objectives for the operational environment can be met
- The TOE is operated in FIPS mode
- Cryptography licences must be obtained and installed
- Users of the TOE should verify the integrity of the TOE firmware before installation. If the firmware version is any other than 1.3.12c the firmware must be updated in accordance with the guidance in [6]. The firmware file name must be pl_1_3_12c.tar with the following SHA-256 checksum: 9d 39 2b 9e 13 3a f8 88 fb e0 e5 d3 d0 8c 23 09 e9 87 61 43 58 60 5e f9 33 1b 35 a1 73 63 fe dc
- Admin and 21 Crypto Officer default passwords MUST be changed at installation time
- Users with the Crypto Officer or Admin roles are strongly encouraged to implement a secure backup mechanism for their credentials. The TOE does not implement a password recovery/reset function
- Users of the TOE are advised to use the latest version of TLS supported by the TOE, which is TLS v1.2.

Annex A – References and abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
4. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
5. *New Zealand Information Security Manual:* https://www.nzism.gcsb.govt.nz/ism-document/
6. Guidance documentation:
   - *PacketLight Networks PL-2000AD 1.3 User Manual – available from the developer*
   - *PacketLight Networks PL-2000ADS 1.3 User Manual – available from the developer*
   - *PacketLight Networks PL-2000M 1.3 User Manual – available from the developer*
   - *PacketLight PL-2000 Series Common Criteria Guidance Supplement v2.2 31 August 2020 – available from the developer*
7. *PacketLight PL-2000 Series with Firmware v1.3.12c Security Target v1.3 dated 31 August 2020*
8. Evaluation Technical Report - *EFT-T010 ETR 1.0 dated 31 August 2020*
9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2-July-2014*
10. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf

Abbreviations

AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CCRA	Common Criteria Recognition Arrangement
EAL	Evaluation Assurance Level
HTTPS	Hypertext Transfer Protocol Secure
LAN	Local Area Network
MSPP	Multi Service Provisioning Platform
OTN	Optical Transport Network
QSFP	Quad Small Form-factor Pluggable

RADIUS	Remote Authentication Dial-In User Service
SFP+	Small Form-factor Pluggable Plus
SSHv2	Secure Shell version 2
TLS 1.2	Transport Layer Security version 1.2
TOE	Target of Evaluation