

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

for

Klas Fastnet Series Switches KlasOS 5.3

Report Number: CCEVS-VR-VID11188-2021
Dated: August 18, 2021
Version: 0.4

National Institute of Standards and Technology
Information Technology Laboratory
101 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell

Randy Heimann

Linda Morrison

Ted Farnsworth

The MITRE Corporation

Common Criteria Testing Laboratory

Dayanandini Pathmanathan

Rodrigo Tapia

Acumen Security, LLC

Table of Contents

1 Executive Summary	5
2 Identification.....	5
3 Architectural Information.....	6
3.1 TOE Product Type	7
3.2 TOE Architecture.....	7
4 Security Policy	9
4.1 Security Audit.....	9
4.2 Cryptographic Operations.....	9
4.2.1 Identification and Authentication	9
4.2.2 Security Management	9
4.3 Protection of the TSF	10
4.4 TOE Access	10
4.5 Trusted Path/Channels	10
5 Assumptions, Threats & Clarification of Scope.....	11
5.1 Assumptions.....	11
5.2 Threats.....	13
5.3 Clarification of Scope.....	16
6 Documentation	16
7 TOE Evaluated Configuration.....	17
7.1 Evaluated Configuration.....	17
7.2 Excluded Functionality	19
8 IT Product Testing.....	20
8.1 Developer Testing	20
8.2 Evaluation Team Independent Testing.....	20
9 Results of the Evaluation	21
9.1 Evaluation of Security Target	21
9.2 Evaluation of Development Documentation.....	21
9.3 Evaluation of Guidance Documents.....	21
9.4 Evaluation of Life Cycle Support Activities	22
9.5 Evaluation of Test Documentation and the Test Activity	22
9.6 Vulnerability Assessment Activity	22
9.7 Summary of Evaluation Results.....	23

10 Validator Comments & Recommendations.....25
11 Annexes26
12 Security Target.....27
13 Glossary28
14 Bibliography28

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Klas Fastnet Series Switches Klas OS 5.3 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in August 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]. 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 provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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.

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). CCTLs evaluate

products against Protection Profiles (PPs) containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

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 Product Compliance List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Klas Fastnet Series Switches KlasOS 5.3
Protection Profile	Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]
Security Target	Klas Fastnet Series Switches KlasOS 5.3 Security Target
Evaluation Technical Report	Evaluation Technical Report for Klas Fastnet Series Switches KlasOS 5.3
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Klas Telecom
Developer	Klas Telecom
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd, Suite 395 Rockville, MD 20850, MD
CCEVS Validators	Paul Bicknell, Randy Heimann, Linda Morrison, Ted Farnsworth

3 Architectural Information

The TOE is the Klas Fastnet Series Switches Klas OS 5.3 (herein referred to as the TOE). It runs the KlasOS firmware, which provides connectivity to multiple devices contained within the same network segment. A real-time clock is present on all KlasOS devices. Authentication can be performed locally or over a trusted channel using SSH. All logs can be securely transferred to a syslog server. KlasOS provides a Command Line Interface (CLI) for device configuration. The Klas Fastnet switches range of products provide expandable, enterprise-grade, rugged mobility solutions.



3.1 TOE Product Type

The TOE is classified as a network device which is composed of hardware and software that offers scalable solutions to its end-users. It satisfies all the criteria needed to meet the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e] requirements.

3.2 TOE Architecture

The TOE consists of the following models:

Table 2: TOE Models

Hardware Platforms	Specifications
<p>Klas Voyager TDC 10G Switch</p> 	<ul style="list-style-type: none"> • 512 GB RAM • 32 Physical CPU Cores • Up to 32 TBs of raw storage • 10 GB/s networking • Ten 10-Gigabit Switch ports (4 available as copper or SFP to support fiber-optic connectivity) • 1 gigabit management port • 1 VIK slot (for removable storage) • 1 console port • Processor: Marvell Prestera 98DX8212 (ARM v7)
Hardware Platforms	Specifications
<p>Klas Voyager TDC 12GG Switch</p> 	<ul style="list-style-type: none"> • Small form factor variant of the Voyager TDC Switch, the first 10 Gb/s switch available for the tactical market • 121 Gb/s backplane for line-speed processing simultaneously on all ports • 40 Gb/s trunk for speeds • 1x 40 Gb/s QSFP+ high-speed uplink port or 4x 10-Gigabit SFP+ ports (based on breakout cable selection) • 8x 1- Gb/s SFP+ ports • 1 Gigabit management port,

- 1 VIK slot (for removable storage)
- 1 console port
- Processor: Marvell Prestera 98DX8212 (ARM v7)

4 Security Policy

The TOE implements the following security functional requirements:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

Each of these security functionalities are covered in more detail below.

4.1 Security Audit

The TOE generates audit events for all start-up and shutdown functions as well as all auditable events specified in Table 13 ‘Auditable Events’ of the ST. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE can store audit records locally and export them to an external syslog server using SSHv2. Each audit record contains the date and time of the event, type of event, subject identity, and other relevant data of the event. Only a Security Administrator can enable logging to a syslog server.

4.2 Cryptographic Operations

The TOE contains CAVP-tested cryptographic implementations that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key hashing features in support of high-level cryptographic protocols including SSH. The operating system used is Klas OS v5.3.5. The TOE leverages OpenSSL 1.0.1u for cryptographic algorithms and OpenSSH 7.7p1 for SSH.

4.2.1 Identification and Authentication

All users must be authenticated by the TOE prior to carrying out any administrative actions. The TOE supports password-based and public-key based authentication. An administrator can set a minimum password length on the TOE which can be a minimum of 15 characters.

4.2.2 Security Management

The TOE supports local and remote management of its security functions including:

- Local console CLI administration
- Remote CLI administration via SSHv2
- Configurable banner displayable at login
- Timeouts to terminate administrative sessions after a set period of inactivity
- Timed user lockout after multiple failed authentication attempts
- Configurable authentication failure parameters
- Re-enabling locked accounts
- Configurable cryptographic parameters

The administrative user can perform all the above security related management functions.

4.3 Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys, and private keys from unauthorized disclosure. Passwords are stored as SHA 512 hashes. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. The TOE internally maintains the date and time. An administrator can install software updates to the TOE after they are verified using a digital signature mechanism.

4.4 TOE Access

The TOE displays a customizable banner before any administrative session can be established with it. The TOE will terminate local or remote interactive sessions after a specified period of session inactivity configured by an administrator. An administrator can terminate their own interactive local or remote sessions.

4.5 Trusted Path/Channels

The TOE supports SSH for secure communications with authorized IT entities such as syslog servers. The TOE supports SSHv2 (remote CLI) for secure remote administration.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

This section describes the assumptions made in identification of the threats and security requirements for Network Devices. The Network Device is not expected to provide assurance in any of these areas, and as a result, requirements are not included to mitigate the threats associated with them. The table below describes conditions which are assumed to exist in the environment where the TOE is deployed. These assumptions are referenced from the PP and remain unchanged from their original source.

Table 3: Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	<p>The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.</p>
A.LIMITED_FUNCTIONALITY	<p>The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).</p> <p>In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.</p>

ID	Assumption
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.

A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
------------------------	--

5.2 Threats

The threats for the Network Device are grouped according to functional areas of the device in the sections below.

Table 4: Threats

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing manin-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and
------------------------------------	---

ID	Threat
	integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes
ID	Threat
	replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

5.3 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e].
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security-related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:



- Klas Fastnet Series Switches KlasOS 5.3 Security Target v1.7 [ST]
- Klas FastNet Series Switches KlasOS 5.3 Common Criteria Configuration Guide v1.0 [AGD]

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE consists of the following models:

Table 5: TOE Models

Hardware Platforms	Specifications
<p>Klas Voyager TDC 10G Switch</p> 	<ul style="list-style-type: none"> • 512 GB RAM • 32 Physical CPU Cores • Up to 32 TBs of raw storage • 10 GB/s networking • Ten 10-Gigabit Switch ports (4 available as copper or SFP to support fiber-optic connectivity), • 1 gigabit management port • 1 VIK slot (for removable storage) • 1 console port. • Processor: Marvell Prestera 98DX8212 (ARM v7)
<p>Klas Voyager TDC 12GG Switch</p> 	<ul style="list-style-type: none"> • Small form factor variant of the Voyager TDC Switch, the first 10 Gb/s switch available for the tactical market • 121 Gb/s backplane for linespeed processing simultaneously on all ports • 40 Gb/s trunk for speeds

	<ul style="list-style-type: none"> • 1x 40 Gb/s QSFP+ high-speed uplink port or 4x 10-Gigabit SFP+ ports (based on breakout cable selection) • 8x 1- Gb/s SFP+ ports • 1 Gigabit management port, • 1 VIK slot (for removable storage) • 1 console port • Processor: Marvell Presteria 98DX8212 (ARM v7)
--	--

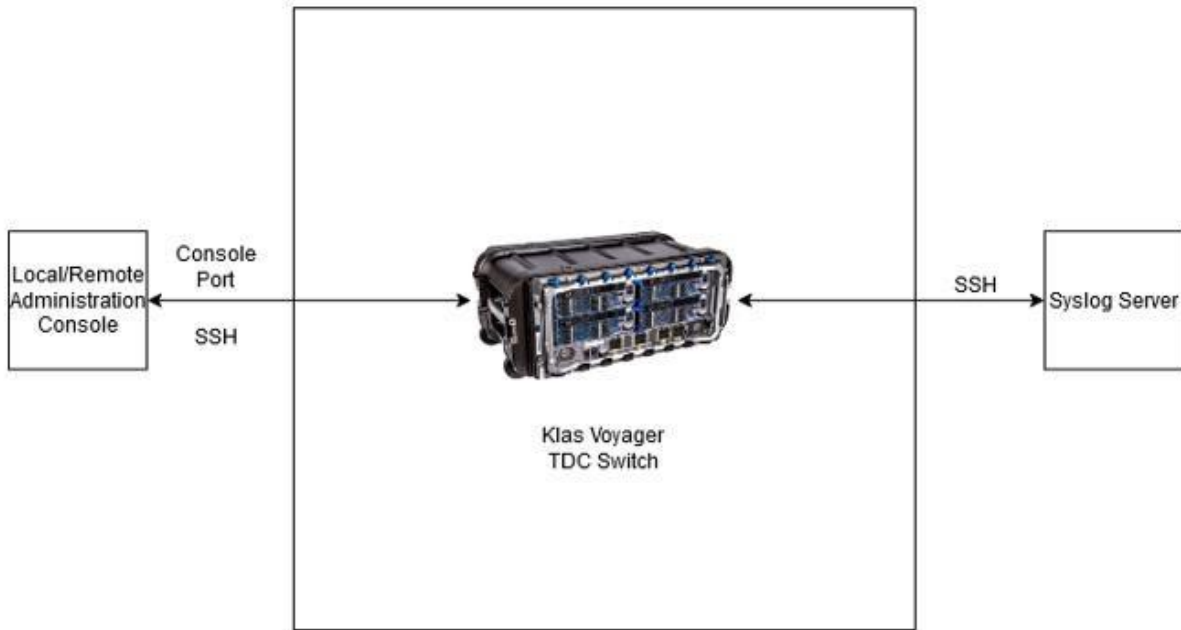
The TOE also supports secure connectivity with several other IT environment devices, including,

Table 6: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation/SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channel. Any SSH client that supports SSHv2 may be used.
Syslog server	Yes	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.

The following is the TOE deployment diagram:

Figure 1: Klas Voyager TDC Deployment Diagram



7.2 Excluded Functionality

The following functionalities are excluded from the evaluation:

Table 7: Excluded Functionality

Excluded Functionality	Exclusion Rationale
SNMP	Not within the scope of evaluation
NTP	Not within the scope of evaluation

The above functions are disabled in the evaluated configuration by default.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Klas Fastnet Series Switches Klas OS 5.3, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that activities and work units received a passing verdict.

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 rev 4 and CEM version 3.1 rev 5. The evaluation determined the Klas Fastnet Series Switches Klas OS 5.3 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Klas Fastnet Series Switches Klas OS 5.3 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e].

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e] related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the Protection Profile for Network Devices, Version 2.2e

[NDcPP v2.2e] related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e] and recorded the results in a Test Report, summarized in the Evaluation Technical Report and AAR.

The validators reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e], and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e], and that the conclusion reached by the evaluation team was justified.

The evaluators documented their analysis and testing of potential vulnerabilities with respect to this requirement.

In compliance with AVA_VAN.1, the evaluators examined sources of publicly available information to identify potential vulnerabilities in the TOE. The sources of examined sources are as follows:

- <https://www.klasgroup.com/>
- <http://nvd.nist.gov/>

- <http://www.us-cert.gov>
- <http://www.securityfocus.com/>
- <https://www.cvedetails.com/>
- www.exploitsearch.net
- www.securiteam.com
- <http://nessus.org/plugins/index.php?view=search>
- <http://www.zerodayinitiative.com/advisories>
- <https://www.exploit-db.com>
- <https://www.rapid7.com/db/vulnerabilities>

The evaluators examined public domain vulnerability searches by performing a keyword search. The terms used for this search were based on the vendor name, product name, and key platform features leveraged by the product. As a result, the evaluator performed a search using the following keywords:

- Klas Telecom
- Klas Switch
- Klas Voyager
- Klas TDC 10G
- Klas TDC 12GG
- KlasOS 5.3.5
- Klas Fastnet Series
- Marvell Prestera 98DX8212
- KlasOS IPv4
- KLAS-VOY-TDC-R2.0
- KlasOS SSH
- KlasOS Syslog
- OpenSSH 7.7p1
- OpenSSL 1.0.1u
- Linux Kernel version 3.10.70
- GNU C Library stable release version 2.13
- Linux-PAM 1.3.1
- rsyslogd 8.34.0

The vulnerability searches were performed on March 24, 2021, May 3, 2021, June 5, 2021, June 24, 2021, and August 5, 2021. No open vulnerabilities applicable to the TOE were identified.

Based on these findings, this assurance activity is considered satisfied.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the document “Klas Fastnet Series Switches KlasOS 5.3 Common Criteria Configuration Guide version 1.0”, dated 9 August 2021. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the Management Workstation, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluation and testing of security functional requirements are scoped by the guidance included by the Assurance Activity associated with the Protection Profile claimed by the TOE. There is an inherent risk that elements of the TOE security functionality were not fully evaluated. It is recommended that the TOE be subject to integration testing within its intended environment to ensure proper configuration, compliance, and operation.

11 Annexes

Not applicable.

12 Security Target

Please see the Klas Fastnet Series Switches KlasOS 5.3 Security Target version 1.7. [ST]

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

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 and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Klas Fastnet Series Switches KlasOS 5.3 Security Target, Version 1.7, 16 July 2021 [ST].
6. Klas Fastnet Series Switches KlasOS 5.3, Common Criteria Configuration Guide, Version 1.0, 09, August 2021 [AGD].
7. Assurance Activity Report for Klas Fastnet Series Switches KlasOS 5.3, Version 0.9, 18 August 2021 [AAR].
8. Evaluation Technical Report for Klas Fastnet Series Switches KlasOS 5.3, Version 0.8, 09 August 2021 [ETR].

9. Vulnerability Assessment for Klas Fastnet Series Switches KlasOS 5.3, Version 0.7, 05 August 2021 [AVA].
10. Test Report for Klas Fastnet Series Switches KlasOS 5.3, Version 1.2, 09, August 2021 [TR].
11. Equivalency Analysis for Klas FastNet Series Switches KlasOS 5.3, Version 0.4, 27 April,2021