National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Kemp LoadMaster

Report Number: **CCEVS-VR-VID11280-2023**

Dated: **01/27/23**

Version: **1.0**

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin
Swapna Katikaneni

Common Criteria Testing Laboratory

Rahul Joshi
Yogesh Pawar
Shaunak Shah
Adarsh Pandey
Yogita Kore

Acumen Security, LLC

Table of Contents

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 Kemp LoadMaster 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 **January 2023**. 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 collaborative Protection Profile for Network Devices Version 2.2e.

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. 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 Security Target (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 containing Assurance Activities, which are interpretation 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 Compliant List.

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	Kemp LoadMaster
Protection Profile	collaborative Protection Profile for Network Devices Version 2.2e
Security Target	Kemp LoadMaster Security Target v0.8
Evaluation Technical Report	Evaluation Technical Report for Kemp LoadMaster v0.4
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Progress Software Corporation
Developer	Progress Software Corporation
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd, Suite 395, Rockville, MD 20850.
CCEVS Validators	Daniel Faigin Swapna Katikaneni

3 Architectural Information

The TOE is Kemp LoadMaster X15, X25 and X40 and Virtual LoadMaster running on OS 7.2.48.8. The LoadMaster simplifies the management of networked resources, and optimizes and accelerates user access to diverse servers, content, and transaction-based systems. The TOE is comprised of hardware and software and represents a complete network device providing load balancing functionality.

The TOE evaluated configuration consists of one of the appliances listed below. The LoadMaster X15, X25 and X40 are physical devices while the Virtual LoadMaster is a virtual machine which runs on ESXi.:

Table 2 IT Environment Components

Model	**LoadMaster X15**	**LoadMaster X25**	**LoadMaster X40**	**Virtual LoadMaster**
Processor	Intel Xeon E3-1275v6 (Kaby Lake)	Intel Xeon 4116 Silver (Skylake)	Intel Xeon 6136 Gold (Skylake)	Intel Xeon E5 (Broadwell)
RAM	32 GB RAM	64 GB RAM	64 GB RAM	2GB (evaluated)
Network	16 1Gb Ethernet 4 10Gb Ethernet Fiber	2 1Gb Ethernet 12 10Gb Ethernet Fiber	2 1Gb Ethernet 12 10Gb Ethernet Fiber	3 1Gb virtual NIC (evaluated)
Platform	LoadMaster OS 7.2.48.8	LoadMaster OS 7.2.48.8	LoadMaster OS 7.2.48.8	LoadMaster OS 7.2.48.8 on ESXi v6.7

The Virtual LoadMaster was tested on an Intel Xeon E5-4620v4 (Broadwell) and ESXi v6.7.

4 Security Policy

The TOE provides the security functionality required by [NDcPP].

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

4.1 Security Audit

The TOE generates audit records for security relevant events. The audit events are associated with the administrator or processes. The audit records are transmitted over TLS to an external audit server.

4.2 Cryptographic Support

The TOE provides following cryptographic services described below.

Table 3 Cryptographic Services

Service	Use
TLS Client	Secure connection to remote syslog servers.
TLS Client	Secure connection to remote LDAP server.
TLS/HTTPS Server	Secures connections with remote administrators.
Verification of Updates	Digital signature verification prior to installing an update.

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below.

Table 4 CAVP Algorithm Testing References

Algorithm	CAVP Cert.	Standard	Operation/Use	SFR
RSA	C2076	FIPS 186-4	RSA 2048 SigVer	FCS_CKM.1
ECDSA	C2076	FIPS 186-4	ECDSA P-256 SigGen, SigVer ECDSA P-256, P-384, P-521 KeyGen, KeyVer	FCS_CKM.1 FCS_COP.1/SigGen
ECDHE	C2076	SP 800-56Ar2	ECDHE P-256, P-384, P-521	FCS_CKM.2
DRBG	C2076	SP 800-90Ar1	CTR_DRBG(AES-256)	FCS_RBG_EXT.1
AES	C2076	FIPS 197 SP 800-38A SP 800-38D	AES in CBC and GCM modes with 128-bit and 256-bit keys	FCS_COP.1/DataEncryption
SHA	C2076	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512	FCS_COP.1/Hash

Algorithm	CAVP Cert.	Standard	Operation/Use	SFR
HMAC	C2076	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	FCS_COP.1/KeyedHash

4.3 Identification and Authentication

The TOE provides password-based and X.509 certificate-based logon mechanisms. This password-based mechanism encores minimum length requirements. The TOE also validates and authenticates X.509 certificates when they are used to identify a remote TLS server or an administrator logging into the TOE.

4.4 Security Management

The TOE provides management capabilities via a Web-based GUI, accessed over HTTPS. Management functions allow the administrators to configure the system, install updates, and manage users.

4.5 Protection of the TSF

The TOE prevents the reading of plaintext passwords and keys. The TOE provides a reliable timestamp for its own use. The reliable timestamp can be set by a security administrator or authenticated NTP. To protect the integrity of its security functions, the TOE implements a suite of self-tests at startup and halts or disables affected functionality if a self-test fails. The TOE ensures that updates to the TOE are authenticated by verifying a digital signature prior to installing any update.

4.6 TOE access

The TOE monitors local and remote administrative sessions for inactivity and either locks or terminates the session when a threshold time period is reached. An advisory notice is displayed at the start of each session.

4.7 Trusted Path/Channels

The TOE initiates a TLS trusted channel with a syslog server and LDAP authentication server (as configured).

The TOE is a TLS/HTTPS server that allows remote administrators to establish a trusted path with the TOE.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 5 Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	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.
A.LIMITED_FUNCTIONALITY	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). 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.
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 ND cPP. 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.

ID	Assumption
	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.
A.VS_TRUSTED_ADMINISTRATOR	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATON	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 6 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 man-in-the-middle attacks, which would provide access to the administrative session, or

ID	Threat
	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 tunnelling 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 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 replacing existing credentials with an attacker's

ID	Threat
	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 Organizational Security Policies

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

Table 7 Organizational Security Policies

ID	Assumption
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

5.4 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 collaborative Protection Profile for Network Devices Version 2.2e.
- Consistent with the expectations of the Protection Profile, 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:

- Configuring LoadMaster for Common Criteria Conformance v0.2
- LoadMaster CLI Interface description 20 September 2022
- Web User Interface(WUI) Configuration Guide 04 October 2022

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated. . Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE boundary consists of one of the appliances listed below. The LoadMaster X15, X25 and X40 are physical devices while the Virtual LoadMaster is a virtual machine which runs on ESXi.:

Model	LoadMaster X15	LoadMaster X25	LoadMaster X40	Virtual LoadMaster
Processor	Intel Xeon E3-1275v6 (Kaby Lake)	Intel Xeon Silver 4116T (Skylake)	Intel Xeon Gold 6136 (Skylake)	Intel Xeon E5 4620 v4 (Broadwell)
RAM	32 GB RAM	64 GB RAM	64 GB RAM	2GB (evaluated)
Network	16 1Gb Ethernet 4 10Gb Ethernet Fiber	2 1Gb Ethernet 12 10Gb Ethernet Fiber	2 1Gb Ethernet 12 10Gb Ethernet Fiber	3 1Gb virtual NIC (evaluated)
Platform	Loadmaster OS 7.2.48.8	Loadmaster OS 7.2.48.8	Loadmaster OS 7.2.48.8	Loadmaster OS 7.2.48.8 on ESXi v6.7

The TOE supports (sometimes optionally) secure connectivity with several other IT environment devices as described below.

Table 8 IT Environment Components

Component	Required	Usage/Purpose Description
Management Workstation	Yes	Workstation providing local console access to the TOE. Workstation providing a browser to connected to the Web User Interface (WUI) over TLSv1.2 or TLSv1.1.
Audit Server	Yes	Syslog server that receives audit logs from the TOE over TLSv1.2 or TLSv1.1.
ESXi Server	Yes (for Virtual LoadMaster)	ESXi v6.7 acting as the hypervisor for Virtual LoadMaster.
LDAP Server	No	Optional authentication server supporting LDAP over TLSv1.2 or TLSv1.1.
NTP Server	No	Optional NTP server supporting SHA-1 integrity verification.

7.2 Excluded Functionality

The following functionality is excluded (disabled) in the evaluated configuration:

- SSH
- Management API
- Administrative Trusted Channels
- IPv6

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 Kemp LoadMaster**, which is not publicly available. The Assurance Activities Report 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 the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices Version 2.2e.

All testing was carried at the Acumen Security office located in 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from December 21, 2020 - December 16, 2022. The Independent Testing configuration is documented in section 4 of the AAR and the test activities are documented in section 6 of 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 Evaluation Technical Report (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 5 and CEM version 3.1 rev 5. The evaluation determined the Kemp LoadMaster 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 Kemp LoadMaster Security Target 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 collaborative Protection Profile for Network Devices Version 2.2e.

The validator 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 EAL 1 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 collaborative Protection Profile for Network Devices Version 2.2e related to the examination of the information contained in the TOE Summary Specification.

The validator 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 EAL 1 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 collaborative Protection Profile for Network Devices Version 2.2e related to the examination of the information contained in the operational guidance documents.

The validator 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 EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator 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 EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices Version 2.2e and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator 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 collaborative Protection Profile for Network Devices Version 2.2e, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 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 validator 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 collaborative Protection Profile for Network Devices Version 2.2e, and that the conclusion reached by the evaluation team was justified.

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 collaborative Protection Profile for Network Devices Version 2.2e, 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 Common Criteria Administrator Guide.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. The excluded functionality is specified in section 7.2 of this report. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Annexes

Not applicable.

12 Security Target

Kemp LoadMaster Security Target v0.8, January 19, 2023

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 5.
5. Kemp LoadMaster Security Target v0.8, January 19, 2023
6. Configuring LoadMaster for Common Criteria Conformance v0.2, January 19, 2023
7. Evaluation Technical Report for Kemp LoadMaster v0.4, January 19, 2023
8. Assurance Activity Report for Kemp LoadMaster v0.4, January 19, 2023