National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Progress LoadMaster, Version 1.0

Report Number: CCEVS-VR-VID11691-2026

Dated: July 8, 2026

Version: 1.0

National Institute of Standards and Technology	**Department of Defense**
Information Technology Laboratory	**ATTN: NIAP, SUITE: 6982**
100 Bureau Drive	**9800 Savage Road**
Gaithersburg, MD 20899	**Fort George G. Meade, MD 20755-6982**

ACKNOWLEDGEMENTS

Validation Team

NIAP

Matt Downey

Johns Hopkins University Applied Physics Laboratory

Farid Ahmed

Russ Fink

Alex Lee

Robert Wojcik

Common Criteria Testing Laboratory

Rupal Gupta

Theo Ajibade

Akshay Jain

Intertek Acumen Security

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 Progress 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 June 2026. 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 of the list of the Collaborative Protection Profile for Network Devices, Version 3.0e [CPP_ND_V3.0E].

The TOE identified in this VR 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 Protection Profile (PP). This VR 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 ETR 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 ETR 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 PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (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 IT 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	Progress LoadMaster
Protection Profile	*Collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E]
Security Target	Progress LoadMaster Security Target, Version 1.7
Evaluation Technical Report	Evaluation Technical Report for Progress LoadMaster, Version 0.6
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)	Intertek Acumen Security Rockville, MD
CCEVS Validators	Matt Downey, Farid Ahmed, Russ Fink, Alex Lee, Robert Wojcik

3 Architectural Information

3.1 TOE Overview

The TOE is the Progress Software Corporation's Progress LoadMaster X25-NG, LoadMaster X40-NG, ECS CM H2 NG, ECS CM H3 NG and Virtual LoadMaster running on LoadMaster OS 7.2.54.18. 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.

3.2 TOE Description

Progress LoadMaster is a load balancer and application delivery controller (ADC) appliance. It is designed to increase the availability, scalability, and security of applications and data centers. The TOE suits all sizes of organizations with integrated hardware acceleration and support for up to 35 million concurrent connections. The TOE is a network device.

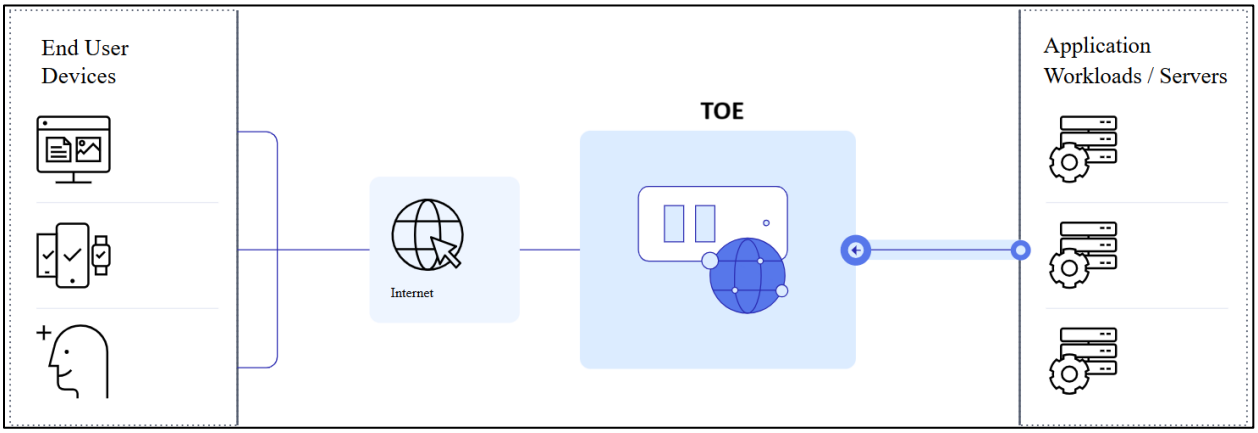

Figure 1 – Representative TOE Deployment

3.3 Physical Boundaries

The TOE boundary consists of one of the appliances listed below. The LoadMaster X25-NG, LoadMaster X40-NG, ECS CM H2 NG and ECS CM H3 NG are physical devices while the Virtual LoadMaster is a virtual machine which runs on ESXi. The virtual TOE is conformant with Case 1 as described in the NDcPP:

Table 2- TOE Physical Boundary Components

Model	LoadMaster X25-NG	LoadMaster X40-NG	ECS CM H2 NG	ECS CM H3 NG	Virtual LoadMaster
Processor	Intel Xeon Silver 4316 (Ice Lake)	Intel Xeon Silver 4316 (Ice Lake)	Intel Xeon Silver 4316 (Ice Lake)	Intel Xeon Silver 4316 (Ice Lake)	Intel Xeon Gold 5222 (Cascade Lake)

Model	LoadMaster X25-NG	LoadMaster X40-NG	ECS CM H2 NG	ECS CM H3 NG	Virtual LoadMaster
RAM	64 GB RAM (evaluated)	64 GB RAM (evaluated)	128 GB RAM	128 GB RAM	4GB (evaluated)
Network	2 1Gb Ethernet 8 10Gb Ethernet Fiber	2 1Gb Ethernet 8 10Gb Ethernet Fiber	2 1Gb Ethernet 8 10Gb Ethernet Fiber 4 25Gb Ethernet Fiber 4 100Gb Ethernet Fiber	2 1Gb Ethernet 8 10Gb Ethernet Fiber 4 25Gb Ethernet Fiber 4 100Gb Ethernet Fiber	2 10Gb virtual NIC (evaluated)
Platform	LoadMaster OS 7.2.54.18	LoadMaster OS 7.2.54.18	LoadMaster OS 7.2.54.18	LoadMaster OS 7.2.54.18	LoadMaster OS 7.2.54.18 on ESXi v7.0 U3

4 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v3.0e or NDcPP.

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 the 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.

4.3 Identification and Authentication

The TOE supports a password-based authentication mechanism which automatically locks users after a pre-configured number of failed attempts. The TOE also validates X.509 certificates in support of TLS.

4.4 Security Management

The TOE provides management capabilities via Console and 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 & Threats

The Security Problem Definition, including the assumptions and threats, can be found in the following documents:

- Collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E]

That information has not been reproduced here and CPP_ND_V3.0E should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V3.0E as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness. A list of excluded functionalities have been documented in Sec 7.2.

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 [CPP_ND_V3.0E].
- This evaluation covers only the specific hardware and software models and versions identified in this document, and not any other models or earlier or later versions released or in process.
- 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 exclusively limited to the functionality specified in the claimed PP. 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:

- Progress Loadmaster Security Target, Version 1.7
- Progress LoadMaster OS 7.2.54.18 Common Criteria Conformance Guide Version 0.5

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.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The following environmental components are required to operate the TOE in the evaluated configuration:

- Management Workstation providing local console access to the TOE and a browser to connect to the Web User Interface (WUI) over TLSv1.2.
- Syslog server that receives audit logs from the TOE over TLSv1.2.
- ESXi v7.0 U3 acting as the hypervisor for Virtual LoadMaster.
- Authentication server supporting LDAP over TLSv1.2.
- NTP server supporting SHA-1 integrity verification with NTPv4.
- OCSP server that receives ocsp requests from TOE over HTTP.
- CA Server that provides signed certificates over HTTP.

7.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- SSH
- Management API
- IPv6
- RADIUS Server

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for Progress LoadMaster, 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 [CPP_ND_V3.0E]. 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 all 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 TOE satisfies the conformance claims made in the Progress LoadMaster Security Target, of Part 2 extended, and Part 3 conformant. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

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 Progress LoadMaster 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 [CPP_ND_V3.0E].

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 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 ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the [CPP_ND_V3.0E] 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 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 [CPP_ND_V3.0E] 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 ALC CEM work unit. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence.

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 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the [CPP_ND_V3.0E] and recorded the results in a Test Report, summarized in the ETR and AAR.

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 [CPP_ND_V3.0E], 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 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 [CPP_ND_V3.0E], 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

[CPP_ND_V3.0E], 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 documentation referenced in Section 6 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. 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.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. This evaluation covers only the specific hardware and software models and versions identified in this document, and not any other models or earlier or later versions released or in process. Other functionality provided by devices in the operational environment, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

Progress LoadMaster Security Target, Version 1.7

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. Assurance Activity Report for Progress LoadMaster, Version 0.5.
2. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
4. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
5. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
6. Evaluation Technical Report for Progress LoadMaster, Version 0.6, June 2026.
7. Progress LoadMaster OS 7.2.54.18 Common Criteria Conformance Guide Version 0.5.
8. Collaborative Protection Profile for Network Devices, Version 3.0e, [CPP_ND_V3.0E].
9. Progress LoadMaster Security Target, Version 1.7.
10. Assurance Activity Report for Progress Loadmaster, version 0.5, June 2026