National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

CAE MPIC 3.0.66

Report Number: CCEVS-VR-11299-2022
Dated: November 23, 2022
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 Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson

Randy Heimann

Lisa Mitchell

Lori Sarem

Ben Schmidt

Chris Thorpe

The MITRE Corporation

Common Criteria Testing Laboratory

Eric Isaac

Kevin Steiner

Lightship Security, USA

Table of Contents

List of Tables

1. Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the CAE MPIC v3.0.66 Target of Evaluation (TOE), performed by Lightship Security USA Common Criteria Laboratory (CCTL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty 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 performed by Lightship Security (LS) of Baltimore, Maryland in accordance with the United States evaluation scheme and completed in November 2022. The information in this report is largely derived from the ST, and the evaluation sensitive documents: Evaluation Technical Report (ETR) and the functional testing report, which are summarized in the Assurance Activity Report. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated April 2017, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 5, April 2017 as well as the assurance activities specified in *Evaluation Activities for Network Device cPP*, Version 2.2, December 2019.

The TOE is a network device used to transmit data from the hardware panels to a software-based flight simulation.

The security functionality specified in the *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 includes protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, ability to verify the source and integrity of updates to the TOE, and use of NIST-validated cryptographic mechanisms.

The Lightship evaluation team determined that the TOE is conformant to the claimed PP. The TOE, when configured as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in *CAE MPIC 3.0.66 Security Target*, Version 1.10, October 2022). The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test report produced by the Lightship evaluation team.

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the

evaluation showed that the TOE satisfies all of the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to the claimed PP, and that the assurance activities specified in the NDcPP had been performed appropriately. Therefore, 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 (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) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 Validated Product Compliant List (PCL).

Table 2 provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product	CAE MPIC v3.0.66
Sponsor and Developer	CAE Inc. 8585, Ch. De la Cote-de-Liesse St-Laurent, QC H4T 1G6
CCTL	Lightship Security USA 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
Completion Date	November 17, 2022
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.
Protection Profile	*collaborative Protection Profile for Network Devices (NDcPP)*, Version 2.2e, March 23, 2020

Item	Identifier
Disclaimer	This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.
Evaluation Personnel	Lightship USA: Eric Isaac, Kevin Steiner
CCEVS Validators	MITRE: Jenn Dotson, Randy Heimann, Lisa Mitchell, Lori Saren, Ben Schmidt, Chris Thorpe

3. Assumptions and Clarification of Scope

3.1. Assumptions

The Security Problem Definition, including the assumptions, can be found in the following document:

- *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020

That information has not been reproduced here and CPP_ND_V2.2E should be consulted if there is interest in that material.

3.2. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V2.2E 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.

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 assurance activities specified in *Evaluation Activities for network Device cPP*, December 2019, Version 2.2 and performed by the evaluation team).

This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.

The evaluation of security functionality of the product was limited to the functionality specified in the ST. Any additional security related functional capabilities of the product were not covered by this evaluation.

This evaluation did not specifically search for, nor attempt to exploit, 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 TOE appliances consist of firmware and hardware and do not rely on the operational environment for any supporting security functionality.

The TOE must be installed, configured and managed as described in the *CAE, Inc. MPIC v3.0.66 Common Criteria Guide*, Version 1.1 to be operated in the evaluated configuration.

4. Security Policy

The TOE enforces the following security policies as described in the Security Target (ST).

Note: Much of the description of the security policy has been derived from the ST.

4.1. Security Audit

The TOE is able to generate audit records of security relevant events. The TOE stores audit records locally and can also be configured to send the audit records to an external audit server over a protected communication channel. Log files are transferred in real time via SSH tunnel to the external audit server. Only authorized administrators may view audit records and no capability to modify the audit records is provided.

4.2. Cryptographic Support

The TOE protects the integrity and confidentiality of communications between itself and the syslog server. The TOE provides the following CAVP-certified cryptographic services: random bit generation; asymmetric cryptographic key pair generation; key establishment; symmetric data encryption and decryption; digital signature generation and verification; cryptographic hashing; and keyed-hash message authentication. When local audit logs reach a maximum size of 8MB, logs are rotated out by removing the oldest log first and creating a new log file.

4.3. Identification and Authentication

The TOE requires all users to be successfully identified and authenticated prior to accessing its security management functions and other capabilities. Administrative access to the TOE is facilitated through the local CLI via direct serial connection or SSH. Administrator credentials are the same for each user regardless of which interface is accessed.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. Only after the administrative user presents the correct authentication credentials will they be granted access to the TOE administrative functionality. Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: !; @; #; $; %; ^; &; *; (; and)

The TOE is capable of tracking authentication failures of remote administrators. When a user account has sequentially failed authentication the configured number of times the account will be locked for a Security Administrator defined time period.

4.4. Security Management

The TOE enables secure management of its security functions, including Administrator authentication with passwords; configurable password policies; Role Based Access Control; access banners; management of critical security functions and data; and protection of cryptographic keys and passwords.

4.5. Protection of the TSF

The TOE protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator.

The TOE provides reliable time stamps for its own use and uses NTP to synchronize its time.

The TOE provides a trusted means for determining the current running version of its firmware and to update its firmware. The TOE verifies the integrity of TOE updates using a hard-coded public key.

The TOE implements various self-tests that execute during the power-on and start up sequence as well as at the administrative user's request, including cryptographic known answer tests that verify the correct operation of the TOE's cryptographic functions.

4.6. TOE Access

The TOE will terminate inactive local and remote interactive sessions after a configurable amount of time. Administrative users may terminate their own sessions at any time using the "exit" command. The TOE displays an administrator configurable message to users prior to login at the CLI.

4.7. Trusted Path/Channels

The TOE protects secure communications with an audit server as a client using SSH. The TOE protects connections from remote administrative users as a server using SSH.

5. Architectural Information

5.1. Physical Scope and Boundary

The TOE is a network device (CAE MPIC v3.0.66) that consists of hardware, software and associated administrator and user guidance. The TOE comprises the hardware, all software and firmware within the network device.

All models have an Cortex-A9 processor and run MPICLinuxDistributionXR 3.0. It comes in a range of form factors MPIC, MPIC-PCMIP, MPIC-EMB. The MPIC-PCMIP form factor differs as it has standard type slot for extensions compared to the custom interface on the MPIC. The MPIC-EMB differs as it is designed to be embedded and not mounted into systems. The differences between the models are not security relevant.

5.2. Required Non-TOE Hardware, Software, and Firmware

The TOE does not require any additional hardware, software or firmware in order to function as a network device. Additional features require that the TOE operates with the following non-TOE components in the environment:

a. Audit Server

b. NTP server services

6. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *CAE Inc. MPIC v3.0.66 Common Criteria Guide,* Version 1.1, October 2022
- *Getting Started with MPIC Developer's Guide TPD 20365 Rev 7,* 20 Oct 2022

All documentation delivered with the product is relevant to and within the scope of the TOE.

7. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *CAE Inc. MPIC v3.0.66 Evaluation Test Report*, which is not publicly available. The *CAE Inc. MPIC v3.0.66 Assurance Activities Report*, Version 0.6, November 2022 provides an overview of testing and the prescribed assurance activities.

7.1. Developer Testing

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

7.2. Evaluation team independent testing

The evaluation team conducted independent testing at Lightship Security USA lab in Austin, Texas. The evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

7.3. Evaluated Configuration

The TOE testing environment components are identified in Table 2 and Table 3 below.

Table 2: Devices in the Testing Environment

Device Name	Protocols	Functions
Syslog Server	SSH	Remote logging server
Remote Workstation	SSH	Remote workstation used for accessing the test environment and SSH administration
Console Laptop	Serial	Laptop used for local console access to the TOE.
MPIC 3.0.66	SSH, NTP	SSH, NTP
Test Server	SSH, NTP	Remote test services server

Table 3: Tools Used for Testing

Tool name	Version	Description
OpenSSH	8.4p1	Used for general purpose SSH CLI access
Wireshark	3.4.4	Used to capture network packets
Lightship Security Greenlight (LS Greenlight)	3.0.35	Used to provide automated support for SSH and NTP protocol testing.
nmap	7.91	Used for IP, TCP and UDP port scanning
OpenVAS	21.04.18	With plugins updated as of 38 days before the publication of this report.

8. 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 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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined the CAE Inc. MPIC v3.0.66 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices (NDcPP).

8.1. 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 CAE Inc. MPIC v3.0.66 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team 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.

8.2. 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 (TSS). Additionally, the evaluator performed the Assurance Activities specified in the NDcPP related to the examination of the information contained in the TSS.

The Validation team 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 the CEM, and that the conclusion reached by the Evaluation team was justified.

8.3. 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.

The Validation team 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 the CEM, and that the conclusion reached by the Evaluation team was justified.

8.4. 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 Validation 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.

8.5. 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 NDcPP and recorded the results in the proprietary Test Report, summarized in the AAR.

The Validation team 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 NDcPP and that the conclusion reached by the Evaluation team was justified.

8.6. Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *CAE Inc. MPIC v3.0.66 NDcPP 2.2e Vulnerability*, Version 0.7, November 2022, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on November 9, 2022, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security: https://www.tenable.com/cve
- Tipping Point Zero Day Initiative: https://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/

- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

The Evaluation team performed a search using the following keywords:

- CAE MPIC
- CAE
- i.MX6
- ARM Cortex-A9
- iptables
- Linux kernel
- openssh
- openssl
- ntpd

The Validation team 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.

8.7. 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 followed the procedures defined in the CEM and performed the Assurance Activities in the NDcPP, and correctly verified that the product meets the claims in the ST.

9. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *CAE MPIC v3.0.66 Common Criteria Guide*, Version 1.1, October 2022 and the *Getting Started with MPIC Developer's Guide, TPD 20365 Rev 7*, 20 October 2022. 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.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

10. Annexes

Not applicable.

11. Security Target

CAE MPIC 3.0.66 Security Target, Version 1.10, October 2022.

12. GLOSSARY

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

14. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Network Devices (NDcPP)*, Version 2.2e, March 23, 2020
6. *Supporting Document Mandatory Technical Document, Evaluation Activities for Network Device cPP*, Version 2.2, December 2019
7. *CAE MPIC 3.0.66 Security Target*, Version 1.10, October 2022
8. *CAE Inc. MPIC v3.0.66 Common Criteria Guide*, Version 1.1, October 2022
9. *Getting Started with MPIC Developer's Guide TPD 20365 Rev 7*, 20 Oct 2022 2021
10. *CAE MPIC 3.0.66 Assurance Activity Report*, Version 0.6, November 2022
11. *CAE MPIC 3.0.66 NDcPP 2.2e Vulnerability Assessment*, Version 0.7, November 2022
12. *CAE MPIC 3.0.66 Evaluation Technical Report*, Version 0.6, November 2022
13. *CAE MPIC 3.0.66 NDcPP 2.2e Test Plan*, Version 0.6, November 2022
14. *CAE MPIC 3.0.66 NDcPP 2.2e Test Results*, Version 0.6, November 2022