National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

3e Technologies International

CyberFence 3e-636 Series Network Security Devices

Report Number:	**CCEVS-VR-11080-2020**
Dated:	**July 14 2020**
Version:	**0.4**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jean Petty, Senior Validator
John Butterworth, Lead Validator
Jenn Dotson, ECR Team
Randy Heimann, ECR Team
Lisa Mitchell, ECR Team
Clare Olin, ECR Team
The MITRE Corporation

Common Criteria Testing Laboratory

John Messiha
Edward Morris
Khai Van
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation Team of the evaluation of CyberFence 3e-636 Series Network Security Devices solution provided by 3e Technologies International. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in July 2020. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019 (NDcPP21).

The Target of Evaluation (TOE) is the CyberFence 3e-636 Series Network Security Devices.

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). 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 monitored the activities of the Evaluation Team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. 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). 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 are consistent with the evidence produced.

The technical information included in this report was obtained from the CyberFence 3e-636 Series Network Security Devices (NDcPP21) Security Target, Version 0.8, 07/06/2020 and analysis performed by the Validation Team.

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) using the Common

Evaluation Methodology (CEM) 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 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 Validated Products 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 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	CyberFence 3e-636 Series Network Security Devices (Specific models identified in Section 3.1)
PP	collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019 (NDcPP21)
ST	CyberFence 3e-636 Series Network Security Devices (NDcPP21) Security Target, Version 0.8, 07/06/2020
Evaluation Technical Report	Evaluation Technical Report for CyberFence 3e-636 Series Network Security Devices, Version 0.4, July 6, 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	3e Technologies International
Developer	3e Technologies International
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Jean Petty, John Butterworth, Jenn Dotson, Randy Heimann, Lisa Mitchell, Clare Olin (all of The MITRE Corporation)

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is CyberFence 3e-636 Series Network Security Devices. The CyberFence 3e-636 Series Network Security Devices TOE is a combination of hardware and software. All devices run software version 5.2.0. The evaluated hardware models are:

- 3e-636L3 EtherGuard
- 3e-636L2 Darknode
- 3e-636H Ultracrypt
- 3e-636A EtherWatch

3eTI's 636 Series Network Security Devices offer the multiple capabilities necessary for protecting embedded devices and safety-critical industrial control systems (ICS) against internal and external attacks. The core capabilities include: network access control, OSI Layer 2 and Layer 3 packet filtering, industrial control protocols packet inspection and secured application data transportation (via encryption).

3.1 TOE Description

The TOE is composed of both hardware and firmware. All four factory configurations of the 3e-636 series devices share identical hardware and a single firmware image. The firmware contains modules, that when activated through manufacture settings, can provide additional functionality specific to each individual device configuration. The 3e-636 runs firmware with naming convention: "signed_dual_636N.5.2.0.00.9.bin". The software version is 5.2.0.

All devices operate in the same operation environment. IPsec tunnels are used to secure the communication between device and external servers such as NTP server and Audit log server. All devices offer the same HTTPS/TLS based GUI interface for device configuration and management

3.2 Physical Boundaries

The TOE physical boundary defines all hardware and firmware that is required to support the TOE's logical boundary and the TOE's security functions. The TOE hardware platform uses FreeScale MPC8378E CPU and the TOE's firmware contains an embedded Linux Kernel customized by 3eTI based on kernel version 4.6. In short, the TOE's physical boundary is the physical device for all models. The TOE provides a dedicated Ethernet interface for local administration as well as additional ports for data traffic.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security Audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF

6. TOE Access
7. Trusted path/channels

4.1 Security Audit

The TOE generates auditable events for actions on the TOE with the capability of selective audit record generation. The records of these events can be viewed within the TOE Management Interface or they can be exported to audit systems in the Operational Environment. The TOE generates records for its own actions, containing information about the user/process associated with the event, the success or failure of the event, and the time that the event occurred. Additionally, all administrator actions relating to the management of TSF data and configuration data are logged by the TOE's audit generation functionality.

4. 2 Cryptographic support

The TOE uses NIST SP 800-90 DRBG random bits generator and the following cryptographic algorithms: AES, RSA, ECDSA, SHA, HMAC to secure the trusted channel and trusted path communication. The TOE is designed to zeroize Critical Security Parameters (CSPs) to mitigate the possibility of disclosure or modification.

4.3 Identification and authentication

The TOE provides Identification and Authentication security functionality to ensure that all users are properly identified and authenticated before accessing TOE functionality. The TOE enforces a password-based authentication mechanism to perform administrative user authentication. Passwords are obscured when being displayed during any attempted login. Administrative users can be authenticated via the TOE's local user database. The TOE also authenticates its IPsec peers; the authentication is performed over IKEv2 SA phase of mutual authentication between IPsec peers.

4.4 Security management

The Web Management Application of the TOE provides the capabilities for configuration and administration. The Web Management Application can be accessed via the dedicated local Ethernet port configured for "out-of-band" management. There is no local access such as a serial console port. Therefore, the local and remote management is considered the same for this evaluation.

An authorized administrator can modify, edit, and delete security parameters such as audit data, configuration data, and user authentication data. The Web Management Application also offers an authorized administrator the capability to manage how security functions behave. For example, an administrator can enable/disable certain audit functions query and set encryption/decryption algorithms used for network packets.

4.5 Protection of the TSF

Internal testing of the TOE hardware, software, and software updates against tampering ensures that all security functions are running and available before the TOE accepts any communications. The TSF prevents reading of pre-shared keys, symmetric keys, private keys, and passwords. The TOE uses electronic signature verification before any firmware/software updates are installed.

4.6 TOE access

The TOE provides the following TOE Access functionality:

- TSF-initiated session termination when a connection (remote or local) is idle for a configurable time period
- Administrative termination of own session
- TOE Access Banners

4.7 Trusted path/channels

The TOE protects interactive communication with administrators using TLS/HTTPS, both integrity and disclosure protection is ensured. The TOE uses IPsec to protect communication with network entities, such as a log server and NTP server. This prevents unintended disclosure or modification of logs and management information.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019 (NDcPP21)

That information has not been reproduced here and the NDcPP21 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP21 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.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 the NDcPP21 and performed by the Evaluation Team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.

7 Documentation

The following document was available with the TOE for evaluation:

- Ultra Electronics 3eTI 636-Series User’s Guide, April 2020, 29000533-002, Revision F

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 to 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.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for CyberFence 3e-636 Series Network Security Devices, Version 0.3, July 6, 2020 (DTR), as summarized in the evaluation Assurance Activity Report.

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 a Common Criteria Certification document and ran the tests specified in the NDcPP21 including the tests associated with optional requirements. The AAR, in sections 1.1 and 3.4.1, lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

9 Evaluated Configuration

See Section 3.1.

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance 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 CyberFence 3e-636 Series Network Security Devices TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP21.

10.1 Evaluation of the Security Target (ASE)

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 CyberFence 3e-636 Series Network Security Devices products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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.

10.2 Evaluation of the Development (ADV)

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 and Guidance documents. Additionally, the Evaluation Team performed the assurance activities specified in the NDcPP21 related to the examination of the information contained in the TSS.

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.

10.3 Evaluation of the Guidance Documents (AGD)

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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

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.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

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.

10.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation Team applied each ATE CEM work unit. The Evaluation Team ran the set of tests specified by the assurance activities in the NDcPP21 and recorded the results in a Test Report, summarized in the AAR.

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.

10.6 Vulnerability Assessment Activity (VAN)

The Evaluation Team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 7/6/2020 with the following search terms: "ultra electronics", "3eti", "darknode", "etherwatch", "etherguard", "ultracrypt", "3e-636", "3e-636L3", "3e-636L2", "3e-636H", "3e-636A", "mpc8378e", "openssl", "Linux Kernel 4.6". No residual vulnerabilities exist in 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 was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

10.7 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 testing 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 correctly verified that the product meets the claims in the ST.

11 Validator Comments/Recommendations

The validation team suggests that the consumer pay particular attention to the installation guidance to ensure the product is placed into the evaluated configuration.

As was noted in the Clarification of Scope section of this report, the product provides more functionality than was covered by the evaluation. Only the functionality claimed in the SFR's in the Security Target was evaluated. All other functionality provided by the product needs to be assessed separately and no further conclusions should be drawn as to effectiveness, nor can any claims be made relative to their security based upon this evaluation.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *CyberFence 3e-636 Series Network Security Devices (NDcPP21) Security Target, Version 0.8, 07/06/2020.*

14 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.

15 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, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019 (NDcPP21)

[5] CyberFence 3e-636 Series Network Security Devices (NDcPP21) Security Target, Version 0.8, 07/06/2020 (ST).

[6] Assurance Activity Report (NDcPP21) for CyberFence 3e-636 Series Network Security Devices, Version 0.4, July 6, 2020 (AAR).

[7] Detailed Test Report for CyberFence 3e-636 Series Network Security Devices, Version 0.3, July 6, 2020 (DTR).

[8] Evaluation Technical Report for CyberFence 3e-636 Series Network Security Devices, Version 0.4, July 6, 2020 (ETR).