National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points

Report Number: CCEVS-VR-11103-2020
Dated: December 21, 2020
Version: 1.0

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

Paul Bicknell
Jenn Dotson
Lisa Mitchell
Linda Morrison
Clare Olin
The MITRE Corporation

Common Criteria Testing Laboratory

John Messiha
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation WiFiProtect 3e-525/523 Series Access Points solution provided by Ultra-3eTI. 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 Columbia, MD, United States of America, and was completed in December 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 EAL 1.

The Target of Evaluation (TOE) is the is Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points.

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 Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points (NDcPP22E/WLANAScEP10) Security Target, Version 0.6, 12/15/2020 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) for Evaluation Assurance Level (EAL) 1 through 4 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	Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points
Protection Profile	collaborative Protection Profile for Network Devices Version 2.2e, 23 March 2020 Network Device Collaborative Protection Profile (NDcPP) Extended Package Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 29 May 2015
ST	Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points (NDcPP22E/WLANAScEP10) Security Target, Version 0.6, 12/15/2020
Evaluation Technical Report	Evaluation Technical Report for Ultra 3eTI WiFiProtect 3e-525/523 Wireless Access Points, Version 0.4, December 15, 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 17
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Ultra 3eTI
Developer	Ultra 3eTI
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	Paul Bicknell, Jenn Dotson, Lisa Mitchell, Linda Morrison, Clare Olin

3 Architectural Information

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

The Target of Evaluation (TOE) is Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points running firmware version 5.1.0. The TOE includes the following hardware models: 3e-525N, 3e-525N MP and 3e-523N. The TOE is classified as a Wireless Local Area Network (WLAN) Access Device.

The TOE sits between wired and wireless portions of an enterprise network and provides integrity and confidentiality of wireless traffic and restricts access of wireless endpoints to wired network systems. The TOE provides a secure, yet flexible, WLAN environment as an Access Point that mediates authenticated wireless client's data through encryption/decryption and integrity protection between the wireless link and the wired LAN.

3.1 TOE Evaluated Platforms

The evaluated TOE is Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points running firmware version 5.1.0. The Target of Evaluation (TOE) includes the following hardware models: 3e-525N, 3e-525N MP and 3e-523N. The models share identical hardware and run the same firmware image.

3.2 TOE Architecture

The 3eTI 3e-525N, 3e-525N MP and 3e-523N Access Points (hereafter referred to as Access Points or APs) provide the connection point between wireless client hosts and the wired network. Once installed as trusted nodes on the wired infrastructure, the APs provide the encryption service on the wireless network between themselves and the wireless clients.

The Access Points are appliances consisting of hardware and firmware. Wireless communications between clients and APs are carried out using the IEEE 802.11 protocol standard. The 802.11 standard governs communication transmission for wireless devices. For this evaluation, the APs use 802.11a, 802.11g and 802.11n for wireless communication. The wireless security protocol that is to be used with the APs is WPA2, which is the Wi-Fi Alliance interoperable specification based on IEEE 802.11i security standard.

The APs have one or more RF interfaces and one or more Ethernet interfaces. All these interfaces are controlled by the firmware executing on the APs. The Access Points included in the TOE vary by the number of RF and Ethernet interfaces and antenna support; however, the differences do not affect the security functionality claimed by the TOE.

The APs maintain a security domain containing all hardware and firmware of the appliance for its own execution. The APs maintain this security domain by controlling the actions that can occur at the interfaces described above and providing the hardware resources that carry out the execution of tasks on the APs. The APs provide for isolation of different

wireless clients that have sessions with the WLAN, which includes maintaining the keys necessary to support encrypted sessions with wireless devices.

The APs control the actions and the manner in which external users may interact with its external interfaces. Thus, the APs ensure that the TOE's enforcement functions are invoked and succeed before allowing the external user to carry out any other security function with or through the APs. The figure below shows the TOE and its operational environment. The trusted path between the TOE and Administration Station is TLS/HTTPS and the trusted path between the TOE and NTP, Log Server and RADIUS server is IPsec.

3.3 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 3.6. In short, the TOE's physical boundary is the physical device/appliance for all models. The APs have the following physical interfaces.

- **AP antenna ports** – The AP antenna ports are connected to one 802.11a/b/g/n radio for wireless connectivity to secure WLAN clients.
- **LAN local port** – The LAN local port is used exclusively for management of the access point. It supports Ethernet 10/100/1000 Mbps wired traffic, full duplex for fast configuration and management. The LAN port is locally terminated – no data entering here goes out to the WLAN, only management data is accepted.
- **WAN uplink port** – The WAN uplink port is intended to connect the 3eTI access points to the wired LAN. It also supports Ethernet 10/100/1000 Mbps wired traffic in a full duplex configuration. The WAN port bridges all data between the wireless domain and the wired network

4 Security Policy

This section summaries 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 Web User

Interface (UI) or they can be exported to audit log servers 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 wireless client data to the LAN, trusted channel and trusted path communication. The TOE zeroizes 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 displays a configurable access banner and enforces a local password-based authentication mechanism to perform administrative user authentication. Passwords are obscured when being displayed during any attempted login.

The wireless users are authenticated by the RADIUS server in the Operational Environment. EAP-TLS is used for WPA2 wireless authentication via x.509 certificates. The TOE sets up an IPsec tunnel with a RADIUS server and supports IKEv2 with x.509 certificates for IPsec endpoints mutual authentication with its IPsec peer.

4.4 Security management

The Web User Interface (UI) of the TOE provides the capabilities for configuration and administration. The Web UI 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 has the ability to modify, edit, and delete security parameters such as audit data, configuration data, and user authentication data. The Web UI 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, firmware, and firmware 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 updates are installed.

4.6 TOE access

The TOE provides the following TOE Access functionality:

- Configurable MAC address and/or IP address filtering with remote management session establishment
- TSF-initiated session termination when a connection is idle for a configurable time period
- Administrative termination of own session
- Configurable MAC address filtering for wireless client session establishment (either allow or deny the client access)
- 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 protects communication with wireless clients using WPA2 with 802.1x EAP-TLS. IPsec tunnels are used by the TOE to setup trusted channels with an NTP, RADIUS and Audit Log server.

5 Assumptions

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

- collaborative Protection Profile for Network Devices Version 2.2e, 23 March 2020
- Network Device Collaborative Protection Profile (NDcPP) Extended Package Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 29 May 2015

That information has not been reproduced here and the NDCPP22E/WLANASCEP10 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 NDCPP22E/WLANASCEP10 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:

- 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.
- The evaluation of security functionality of the product was limited to the functionality specified in the Security Target [6], in the NDcPP and applicable Technical Decisions. Any additional security related functional capabilities included in 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 must be installed, configured and managed as described in the documentation referenced in Section 7 of this Validation Report.

7 Documentation

The following documents were available with the TOE for evaluation:

- WiFiProtect® 3e-520 Series User's Guide, 15 December 2020, 29010012-001, Revision M

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 Detailed Test Report for Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points, Version 0.4, December 15, 2020 (DTR).

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 NDCPP22E/WLANASCEP10 including the tests associated with optional requirements.

9 Evaluated Configuration

The evaluated TOE is Ultra 3eTI WiFiProtect 3e-525/523 Wireless Access Points running firmware version 5.1.0. The Target of Evaluation (TOE) includes the following hardware models: 3e-525N, 3e-525N MP and 3e-523N. The models share identical hardware and run the same firmware image.

To use the product in the evaluated configuration, the product must be configured as specified in the following documents.

- WiFiProtect® 3e-520 Series User's Guide, 15 December 2020, 29010012-001, Revision M

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.

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.

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 Ultra 3eTI WiFiProtect 3e-525/523 Wireless Access Points products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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.

10.2 Evaluation of the Development (ADV)

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 evaluator performed the assurance activities specified in the NDCPP22E/WLANASCEP10 related to the examination of the information contained in the TSS.

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.

10.3 Evaluation of the Guidance Documents (AGD)

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 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.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

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.

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

The evaluation team ran the set of tests specified by the assurance activities in the NDCPP22E/WLANASCEP10 and recorded the results in a Test Report, summarized in the AAR.

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.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team performed a public search for vulnerabilities at the following sites and did not discover any public issues with the TOE. The evaluator searched the following sources for vulnerabilities:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search),
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/),
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities),
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories),
- Exploit / Vulnerability Search Engin (http://www.exploitsearch.net),
- SecurITeam Exploit Search (http://www.securiteam.com),
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search),
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The terms used for the search on 12/02/2020 were as follows"ultra electronics", "3eti", "3e-525N", "3e-525N MP", "3e-523N", "mpc8378e", "fips object module", "tcp", "linux kernel 3.6", "openssl 1.0.2k", "tls", "ipsec", "ike", "wireless access point", "airguard".

Additionally the evaluation team addressed the iTC proposed vulnerability explained in the Bleichenbacher paper. The evaluation team ran the cited tool and the TOE was not vulnerable to the attack.

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.

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 notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the WiFiProtect® 3e-520 User's Guide, 15 December 2020, 29010012-001, Revision M. No versions of the TOE and software, either earlier or later were evaluated.

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

12 Annexes

Not applicable

13 Security Target

Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points (NDcPP22E/WLANAScEP10) Security Target, Version 0.6, 12/15/2020

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, 24 September 2018 (CPP_ND_V2.1),

[5] Network Device Collaborative Protection Profile (NDcPP) Extended Package Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 29 May 2015 (WLANASEP10)

[6] Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points (NDcPP22E/WLANAScEP10) Security Target, Version 0.6, 12/15/2020 (ST)

[7] Assurance Activity Report for Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points, Version 0.4, December 15, 2020 (AAR)

[8] Detailed Report for Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points, Version 0.4, December 15, 2020 (DTR)

[9] Evaluation Technical Report for Ultra 3eTI WiFiProtect 3e-525/523 Series Wireless Access Points, ETR, Version 0.4, December 15, 2020 (ETR)