National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

General Dynamics Mission Systems

Fortress Mesh Point ES210, ES520, ES820, ES2440 Security Target (Wireless LAN Capabilities)

Report Number: CCEVS-VR-VID10777-2016
Dated: **5/31/2016**
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 Panel

Mr. Daniel Faigin
Ms. Marybeth Panock

The Aerospace Corporation
El Segundo, CA

Mr. Kenneth Stutterheim
The Aerospace Corporation
Columbia, MD

Mr. Luke Florer
The Aerospace Corporation
Chantilly, VA

Common Criteria Testing Laboratory

Brad Mitchell, Michael Baron
InfoGard Laboratories, Inc.
San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the Fortress Mesh Point ES210, ES520, ES820, ES2440 devices.

This report is intended to assist the end-user of this product with determining the suitability of this 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.

The TOE is classified as a Wireless Local Area Network (WLAN) Access Device. The TOE employs Mesh networking, which allows multiple TOEs to network within the operational environment. Only WLAN functionality is evaluated in this Security Target. All VPN Gateway functionality was evaluated in a separate Security Target under vid10667.

Table 1 below identifies components that must be present in the Operational Environment to support the operation of the TOE:

Component	Description
Syslog Server	External IT entity for audit log storage and review. • Compatible with RFC 3164 • Supporting IPsec as defined in ST Section 6.1.2.11 FCS_IPSEC_EXT.1 IPsec
NTP Server	External IT entity for accurate time accounting. • V4 conformant to RFC 5905 with a SHA-1 authentication[1].

Remote Management (GUI)	Web Browser (the TOE is known to be compatible with the following web browsers):
	• Firefox v3.6 to 44.0.2
	• IE version 7.0-10.0
	• Compatible with HTTPS implementing:
	  • HTTPS protocol that complies with RFC 2818
	  • TLS 1.0 (RFC 2246)
	  • Compatible with TLS using the following:
	  • Mandatory cipher suites:
	  ○ TLS_RSA_WITH_AES_128_CBC_SHA
	  • Optional cipher suites:
	  ○ TLS_RSA_WITH_AES_256_CBC_SHA
	  ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA
	  ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Remote Management (SSH)	• V2 client compatible with the list of required ciphers (as listed in ST Section 6.1.2.13 FCS_SSH_EXT.1 SSH).

[1] SHA-1 authentication for NTP was not evaluated and therefore cannot claim any cryptographic security.

Local Console	• RS-232 Console Port compatible with the following enumeration settings: o bits per second: 9600 o data bits: 8 o parity: none o stop bits: 1 o hardware flow control: none
Ethernet	• 10BASE-T/100BASE-TX Base Ethernet
Wireless Client Hardware/Firmware	• Wireless 2.4GHz, 4.4GHz, 4.9GHz, or 5.0GHz, IEEE 802.11 a/b/g/n (depending on radio see ST Section 1.4.1.1 for Radio Configuration) • WPA2 (a security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks)
Antenna(s)	• ES210 and ES2440 Specific (not in ES520, 820): o GPS antenna with SMA connector • Wifi Antenna with N-style connector • Capable of transmitting and receiving on the required frequency as described by ST Section 1.4.1.1 for Radio Configuration.
Authentication Server (RADIUS)	• Compatible with RFC 2865 • Supporting IPsec as defined in ST Section 6.1.2.11 FCS_IPSEC_EXT.1 IPsec.

Table 1: Operational Environment Components

2 Identification of the TOE

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 organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Fortress Mesh Point: ES210-3 810-00020-01 ES210-4 810-00029-01 ES2440-0 810-00046-01 ES2440-34 810-00050-01 ES2440-3444 810-00038-01

	ES2440-3444m 810-00060-01 ES2440-34m 810-00061-01 ES2440-35 810-00051-01 ES2440-3555 810-00037-01 ES520-34 810-00022-01 ES520-35 810-00015-01 ES820-34 810-00030-01 ES820-35 810-00023-01 All running Software Version: 5.4.5.2240
Protection Profile	Wireless Local Area Network (WLAN) Access Systems Protection Profile, Version 1.0, December 1, 2011
Security Target	Fortress Mesh Point ES210, ES520, ES820, ES2440 Security Target
Dates of Evaluation	April 19, 2016 – May 31, 2016
Conformance Result	Pass
Common Criteria Version	CC Version 3.1r3, July 2009
Common Evaluation Methodology (CEM) Version	CEM Version 3.1r3, July 2009
Common Evaluation Methodology (CEM) Version	CEM Version 3.1r4, September 2012
Evaluation Technical Report (ETR)	Common Criteria Evaluation Technical Report, 16-3723-R-0018 V1.3, May 31, 2016
Sponsor/Developer	General Dynamics Mission Systems
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc. NVLAP Lab Code: 100432-0
CCTL Evaluators	Brad Mitchell, Michael Baron
CCEVS Validators	Daniel Faigin, Marybeth Panock, Luke Florer, Kenneth Stutterheim

Table 1: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before November 27, 2015.

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

- Security Audit (FAU)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Protection of the TSF (FPT)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

The TOE includes the following functionality that is not covered this Security Target and the associated evaluation:

- VPN Gateway functionality (evaluated in a separate evaluation)
- GPS
- DHCP server
- DNS services
- QoS
- VLANs
- Mobile Security Protocol (MSP)
- Device Access Control
- Fortress Mesh Viewer Protocol
- Layer 2 link management (e.g. Spanning Tree Protocol)

These features may be used in the evaluated configuration; however, no assurance as to the correct operation of these features is provided, modulo those capabilities covered in separate evaluations.

4.1 Security Audit

The TOE has the ability to audit events based on a specified criteria. To protect the TSF from audit log overflow, the TOE uploads audit data to an external syslog server through an IPsec tunnel. The audit record includes: the date and time of the event, the user who triggered the event (if event was user based and user is known), and event specific information. A subset of auditable events required by the ST is found in ST Section 6.1.1.1 FAU_GEN and ST Section 7.3, Table 11 – Audit Record Events. The TOE also protects all locally stored audit data from un-authorized modification and deletion. The TOE implements SyslogD version 1.5.0.

4.2 Cryptographic Operations

The TOE provides cryptographic functions to protect information, including mechanisms to encrypt, decrypt, hash, digitally sign, and perform cryptographic key agreement. The evaluated configuration uses a subset of the cryptographic implementations listed in ST Section 9 for all cryptographic purposes. The FIPS-Approved cryptographic algorithms used by the TOE, and specified by the SFRs, are listed in ST Appendix B, Table 15. The following protocols are implemented by the TOE and use FIPS-Approved cryptographic algorithms:

- WPA2 (IEEE 802.11i)
- WPA2 (EAP-TLS)
- IPsecTLS1.0/HTTPS
- SSHv2
- HTTPS/TLS

4.3 User Data Protection

The TOE protects user data, (i.e., only that data exchanged with wireless client devices), using the IEEE 801.11i standard wireless security protocol. The TOE mediates the flow of information passing to and from the WAN port and ensures that resources used to pass network packets through the TOE do not contain any residual information.

4.4 Identification and Authentication

The TOE requires the system administrators to be authenticated before access to the TOE is granted; administrators may login to the TOE by providing a user name and password via a local RJ45 using a serial RS-232 connection, and via SSH, HTTPS, or X.509 for TLS. Administrators may connect to the TOE remotely via the LAN, WAN, or 802.11a/b/g/n interfaces.

The TOE displays a configurable access banner and requires an administrator to authenticate using a username and password. An external RADIUS server can be configured for authentication through an IPsec tunnel. Authentication can take place, by user name and password (and hexadecimal device ID if applicable). For IPsec, the TOE also supports X.509 certificates. EAP-TLS is used for WPA2 wireless authentication via x.509 certificates.

4.5 Security Management

The management of the security relevant parameters of the TOE must be performed by the authorized administrator; the TOE provides the following management interfaces:

- Command Line Interface (CLI) via
  - Local RJ45 or serial connection,
  - Remote SSH interface via the LAN, WAN ports, and IEEE 802.11 wireless interface
- Remote HTTPS Web UI via the LAN, WAN ports, and IEEE 802.11 wireless interface

4.6 Protection of the TSF

The TOE identification and authentication security functions allow only authenticated administrative users direct access to the TOE. If a wireless user does not authenticate as an

administrative user then that user is a wireless client and can only pass traffic through the TOE and cannot execute commands on the TOE.

Administrative users are allowed to login via the CLI and Web UI to access all management functions. The management interfaces do not allow administrative users access to the underlying operating system and there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE. Any access to a management interface (CLI or GUI) is protected by a secure channel except via RS-232; as this is considered local administration.

The TOE has the capability to obtain reliable time from a remote Network Time Protocol (NTP) Server to provide reliable time stamps for audit services. Additionally, the system administrator can manually set the time (maintained locally in the hardware Real Time Clock (RTC)) on the TOE using the Web UI or CLI management interfaces.

The TOE runs a set of self-tests on power-on to verify the correct operation of the TOE's underlying hardware, TOE software and cryptographic modules. Additional cryptographic tests are performed during normal operation. The security of network data is maintained by ensuring no residual information is included in network packets.

4.7 TOE Access

The TOE displays the access banner before establishing an administrative session. The TOE terminates an interactive session after an Authorized Administrator-configurable time interval of session inactivity. A wireless client session is defined as being allowed access to a particular port on the application layer. The TOE is able to deny establishment of a wireless client session based mac address.

4.8 Trusted Path/Channels

The TOE uses IEEE 802.11-2007 and IPsec to provide a trusted communication channel between itself and any authorized IT entities. In addition to IPsec, EAP-TLS is used for RADIUS.

The TSF initiates communication via the trusted channel for RADIUS, NTP and Syslog. The TOE uses SSH and TLS/HTTPS to provide a trusted communication path between itself and remote administrators.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the

	environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
A.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.
T.RESOURCE_EXHAUSTION	A process or user may deny access to TOE services by exhausting critical resources on the TOE.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.
P.COMPATIBILITY	The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate inter-operation with other network equipment (e.g., certificate authority, NTP server) using the same protocols.

P.EXTERNAL_SERVERS	The TOE must support standardized (RFCs) protocols for communication with a centralized audit server and a RADIUS authentication server.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.

5.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. 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 claimed PP and performed by the evaluation team).
2. This evaluation covers only the specific software/firmware version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. 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.
5. This evaluation covers only the WLAN functionality as specified by the WLANPP. All other features and capabilities were not evaluated and no conclusions can be drawn as to their effectiveness or correct operation when the device is configured in the evaluated configuration.
6. This evaluation reused testing evidence from VID 10667, Fortress Mesh Point ES210, ES520, ES820, ES2440. That validation covered the same product, but was evaluated against the Network Device Protection Profile with the VPN EP. Testing evidence was reused for those SFRs where the requirement and the assurance activity was the same. The two validations shared configuration guidance, ensuring the products were in the same configuration. The original VID10667 validation was against a slightly earlier version of the firmware. The CCTL submitted a maintenance against VID10667 to bring it to the same firmware as this validation. The ACMR, indicating that the change was minor and providing details on the regression testing performed, is being issued concurrent with this VR.

6 Architectural Information

The TOE is classified as a Wireless Local Area Network (WLAN) Access Device for Common Criteria purposes. The TOE is made up of hardware and software components.

6.1 Architecture Overview

The TOE consists of hardware and software components.

6.1.1 TOE Hardware

The TOE hardware components are described as follows:

6.1.1.1 TOE Processor Identification

Table 3 – TOE Processor Identification

Model	Processor	Crypto Accelerator
ES210	AMD Alchemy AU1550	Xilinx Spartan FPGA
ES820	AMD Alchemy AU1550	Xilinx Spartan FPGA
ES520	AMD Alchemy AU1550	Xilinx Spartan FPGA
ES2440	Broadcom XLS416	Xilinx Spartan FPGA

6.1.1.2 TOE Ethernet Port Summary

Table 4 – TOE Ethernet Port Summary

Model	# of Eth Ports	HW Label	GUI Label	Takes PoE	Serves PoE
ES210	2	Ethernet (WAN)	Ethernet1	no	no
		Ethernet	Ethernet2	no	no
ES820	2	Enet1/P1	Ethernet1	no	no
		Enet2/P2	Ethernet2	no	no
ES520	9	WAN	wan1	yes	no
		1–8	lan1–lan8	no	yes
ES2440	3	Ethernet1/WAN/POE	Ethernet1	yes	no
		Ethernet2	Ethernet2	no	no
		Ethernet3	Ethernet3	no	no

6.1.1.3 Radio Configurations

The TOE radio modules are logically identical and have no implications on security or functionality except the frequency and the link layer (layer 1 on the OSI stack) which are specific to the radio. Within each unique identifier there is a primary model number (i.e., ES2440) followed by a dash and then a digit (i.e., 3, 4, or 5).

- Radio ‘3’ - 250mW frequencies 2.4GHz, 4.9GHz and 5GHz using 802.11a/b/g/n
- Radio ‘4’ - 600mW frequency 4.4GHz and 802.11 a/n
- Radio ‘5’ - 500mW frequencies 4.9GHz, 5GHz using 802.11 a/n

6.1.1.4 ES210

The ES210 acts as a layer 2 bridge with VPN functionality and a wireless access point. The ES210 can operate at the given frequencies and data link protocols listed above in Section 6.1.1.3 – Radio Configurations. The physical boundaries of the ES210 are at all of the connectors of the TOE module:

- RJ45 10/100BT Ethernet Port (2)
- 3 Pin Con-X Serial Connector (3 pin mil-spec round connector)
- 2 Pin Con-X Power Connector (2 pin mil-spec round connector)
- RP-TNC Antenna Connector (1)
- SMA Connector

Indicators are used to allow the operator to have a quick indication of the state of the ES210:

- Power
- Battery
- Ethernet1/Ethernet 2 – Link/Activity
- Radio activity

The ES210 also has the following physical button controls:

- Power On/Off
- Blackout Mode
- RF Kill
- Zeroize

6.1.1.5 ES520

The ES520 acts as a layer 2 bridge with VPN functionality and a wireless access point. The ES520 can operate at the given frequencies and data link protocols listed above in Section 6.1.1.3 – Radio Configurations. The physical boundaries of the ES520 are at all of the connectors of the TOE module:

- RJ45 10/100BT Ethernet Port (8)
- USB Host Connector
- 10/100BT WAN Port (1)
- 3 Pin Con-X Serial Connector (3 pin mil-spec round connector)
- DC Power Input Connector
- N-type Antenna Connector (2)

Indicators are used to allow the operator to have a quick indication of the state of the ES520:

- Power
- Clr
- Status 1
- Status 2
- Fail
- Radio1/Radio2 (Upper)

- Radio1/Radio2 (Lower)

The ES520 also has the following controls:

- Reset Button

6.1.1.6 ES820

The ES820 acts as a layer 2 bridge with VPN functionality and a wireless access point. The ES820 can operate at the given frequencies and data link protocols listed above in Section 6.1.1.3 – Radio Configurations. The physical boundaries of the ES820 are at all of the connectors of the TOE module:

- MIL Connector; includes the following interfaces:
  - RJ45 10/100BT Ethernet Port (2)
  - USB
  - Serial
  - All LED indicators
  - All Controls
- 3 Pin Con-X Serial Connector (3 pin mil-spec round connector)
- N-type Antenna Connector (2)

Indicators are used to allow the operator to have a quick indication of the charge state of the ES820. The following indicators are available through the MIL connector:

- Power
- Status
- Ethernet1/Ethernet 2 – Link/Activity
- Radio activity

The ES820 has the following input functions by means of the MIL connector:

- Power On/Off
- Blackout Mode
- RF Kill
- Reset
- Zeroize

6.1.1.7 ES2440

The ES2440 acts as a layer 2 bridge with VPN functionality and a wireless access point. The ES2440 can operate at the given frequencies and data link protocols listed above in section 6.1.1.3 – Radio Configurations. The physical boundaries of the ES2440 are at all of the connectors of the TOE module:

- RJ45 10/100/1000BT Ethernet Port (3)
- RJ45 Serial Connector
- 2 Pin Con-X Power Connector (2 pin mil-spec round connector)
- N-type Antenna Connector (8)
- SMA Connector

Indicators are used to allow the operator to have a quick indication of the state of the ES2440:

- Power
- Ethernet1/Ethernet 2/Ethernet3 link/activity – Link/Activity
- Radio1/Radio2/Radio3/Radio4 activity

The ES2440 also has the following physical button controls:

- Recessed Button

6.1.2 TOE Software/Firmware Version

The TOE firmware is version:

- 5.4.5.2240

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the TOE.

7.1 Guidance Documentation

Document	Revision	Date
Fortress Common Criteria Operational Guidance	1.8	April 27, 2016
Fortress Mesh Point and Network Encryptor Software CLI Guide	009-00036–00v5.4.5	2015
Fortress Mesh Point and Network Encryptor Software GUI Guide	009-00035-00v5.4.5	2015

7.2 Test and Vulnerability Assessment Documentation

Document	Revision	Date
Fortress WLAN Test Plan	V1.4	May 31, 2016

7.3 Security Target

Document	Revision	Date
Fortress Mesh Point ES210, ES520, ES820, ES2440 Security Target	2.5	May 27, 2016

8 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

8.1 Evaluation Team Independent Testing

The CCTL (InfoGard Laboratories, Inc.) generated the testing plan and designed the testing activities specified in the Wireless Local Area Network (WLAN) Access Systems Protection Profile, Version 1.0, December 1, 2011, and generated automated and manual tests to execute the designed test plan. For those tests and assurance activities that were congruent with the NDPP+VPN validation, the evaluation team verified the product conformities during the period September 8, 2015 – January 26, 2016 at the CCTL according to the Fortress Mesh Point ES210, ES520, ES820, ES2440 Security Target (VPN Evaluation), Version 1.5, February 18, 2016, and ran the tests specified in the Protection Profile for Network Devices v1.1, June 8, 2012, the Security Requirements for Network Devices Errata #3, November 3, 2014, and the Network Device Protection Profile Extended Package VPN Gateway, Version 1.1, April 12, 2013 documents.

The WLAN specific validation testing was performed in April 2016. Testing was performed at InfoGard Laboratories in San Luis Obispo, CA for all tests other than FRU_RSA.1 "Maximum Quotas". Due to the specialized hardware needed to adequately validate the claim in [ST] Section 6.1.7.1, testing for this element was performed by GDMS engineers at their facility in Massachusetts. The evaluator reviewed their findings for consistency and accuracy, and found it sufficient. The evaluation also ensured that the vendor testing used the configuration called out in the CC configuration documentation. The validation team reviewed the argument for this exception to the testing policy and found it acceptable, and the evidence demonstrated that the results would have been the same had the team been present for the test.

The test configurations and tools used to evaluate the TOE for both the WLAN and VPN validations were the same, modulo differences required for testing, and are described in the Assurance Activity Report (AAR) Section 5, "Testing Environment".

8.2 Vulnerability Analysis

All testing assurance activities and vulnerability assessment (AVA_VAN) activities were performed against the TOE by the CCTL.

The CCTL has developed a custom testing environment for evaluations which uses several virtual machines, isolated networks, and smart switches in order to meet the requirements stated by the testing assurance activities.

For the Wireless Local Area Network (WLAN) Access Systems Protection Profile, the evaluator performed a vulnerability survey using CVEdetails.com in order to discover any publicly available exploits. The evaluator searched CVEdetails.com for the following keywords:

- Fortress
- General Dynamics
- ES2400, ES820, ES520, ES210
- MeshPoint (+ "Router")

Each search returned no relevant results.

The vendor provided the following table of third-party network modules. The evaluator searched cvedetails.com on April 20, 2016, for vulnerabilities related to each module, with the following results:

Library/3rd Party Module	Version	Disposition	Vulnerability Summary
Fortress Cryptographic Implementation (SSL)	2.1	No vulnerabilities found.	N/A
Fortress Cryptographic Implementation (FPGA)	2.0	No vulnerabilities found.	N/A
Openssl SSL lib	1.0.1i	Found vulnerabilities.	Vulnerabilities found for OpenSSL were not applicable to the TOE because the TOE did not use or support the vulnerable feature, mitigates the vulnerability by various means, or is not applicable to the TOE functionality.
Openssl crypto lib and FIPS module	2.0.9	No relevant findings – FIPS module is used internally, and is not network accessible.	
NTP server & client	4.2.6	No vulnerabilities found related to this version.	N/A
Mocana IKE/Cryptographic lib	5.3.1	No vulnerabilities found.	
Dnsmasq (DNS and DHCP)	2.57	No vulnerabilities found related to this version.	
avahi-daemon (mDNS)	0.6.31	No vulnerabilities found related to this version.	
OpenSSH	5.8p1	Found vulnerabilities.	Vulnerabilities found for OpenSSH were not applicable to the TOE because the TOE did not use or support the vulnerable feature, mitigates the vulnerability by various means, cannot be configured to the vulnerable state, or is not applicable to the TOE functionality.
NET-SNMP	5.4.2.1	Found vulnerabilities.	The vulnerability found for NET-SNMP was not applicable to the TOE because for this vulnerability to be relevant, the TOE would require configuration that would take it out of the CC evaluated configuration.
Apache (HTTPS server)	2.2.23	Found vulnerabilities.	Most of the vulnerabilities found for Apache were not applicable to the TOE because the TOE did not use or support the vulnerable feature, mitigates the vulnerability by various means, cannot be configured to the vulnerable state, or is not applicable to the TOE functionality. The remaining vulnerability consists of a low severity Denial Of Service vulnerability that does not subvert the integrity or security of the TOE and the TOE has mitigations to reduce the probability of and to recover from such an attack should it be successful, via watchdog rebooting of the service affected or of the TOE itself.
Apache PHP library (libphp5.s0)	5.3.1	Found vulnerabilities.	

FreeRADIUS	2.1.12	Found vulnerabilities.	Vulnerabilities found for FreeRADIUS were not applicable to the TOE because the TOE did not use or support the vulnerable feature, mitigates the vulnerability by various means, cannot be configured to the vulnerable state, or is not applicable to the TOE functionality.
Dibbler (IPv6 DHCP server)	0.8.0	No vulnerabilities found related to this version.	N/A
Hostapd	0.7.3	Found vulnerabilities.	All of the vulnerabilities found for Hostapd were not applicable to the TOE because the TOE did not use or support the vulnerable feature, mitigates the vulnerability by various means, cannot be configured to the vulnerable state, or is not applicable to the TOE functionality.
wpa_supplicant	0.7.3	Found vulnerabilities.	All of the vulnerabilities found for wpa_supplicant were not applicable to the TOE because the TOE did not use or support the vulnerable feature, mitigates the vulnerability by various means, cannot be configured to the vulnerable state, or is not applicable to the TOE functionality.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.

InfoGard has determined that the TOE meets the security criteria in the Security Target, which claims compliance with the Wireless Local Area Network (WLAN) Access Systems Protection Profile, Version 1.0, December 1, 2011.

A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in May 2016.

10 Validator Comments/Recommendations

As was noted in the Clarification of Scope section of this report, the devices provide 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 devices needs to be assessed separately and no further conclusions should be drawn as to their effectiveness, nor can any claims be made relative to their security based upon this evaluation.

11 Security Target

Fortress Mesh Point ES210, ES520, ES820, ES2440 Security Target, version 2.5, May 27, 2016.

12 Terms

12.1 Acronyms

CC	Common Criteria
CCTL	Common Criteria Testing Laboratory
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 3, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.

[5] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, September 2012, Version 3.1, Revision 4, CCMB-2009-07-004

[6] Wireless Local Area Network (WLAN) Access Systems Protection Profile, Version 1.0, December 1, 2011.

[7] Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1 April 12, 2013

[8] Fortress Mesh Point ES210, ES520, ES820, ES2440 Security Target v1.6 (VPN Capabilities)