National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Adtran's FSP 3000R7 Network Element r22.2.2

Report Number: CCEVS-VR-VID11418-2024
Dated: March 28, 2024
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
Lisa Mitchell
Linda Morrison
Lori Sarem
The MITRE Corporation

Russell Fink
Bryan Major
Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Christopher Rakaczky
Evan Seiz
Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of Adtran's FSP 3000R7 Network Element operating with software release 22.2.2. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in March 2024. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the *collaborative Protection Profile for Network Devices Version 2.2e* (NDcPP22e).

The TOE is Adtran's FSP 3000R7 Network Element r22.2.2, also referred to as the FSP 3000R7 from this point forward. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR 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 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Adtran's FSP 3000R7 Network Element r22.2.2 Security Target v1.0*, dated January 10, 2024, 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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	Adtran's FSP 3000R7 Network Element r22.2.2
Protection Profile	*collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020
Security Target	*Adtran's FSP 3000R7 Network Element r22.2.2 Security* Target, v1.0, January 10, 2024
Evaluation Technical Report	*Adtran's FSP 3000R7 Network Element r22.2.2 Evaluation Technical Report*, v1.0, March 17, 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Adtran Networks North America, Inc.
Developer	Adtran Networks North America, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
Evaluation Personnel	Herbert Markle, Christopher Rakaczky, Evan Seiz
CCEVS Validators	Jenn Dotson, Lisa Mitchell, Linda Morrison, Lori Sarem, Russell Fink, Bryan Major

3 Architectural Information

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

The TOE is Adtran's FSP 3000R7 Network Element operating with software release 22.2.2. The TOE is an optical network management tool. The product is a scalable optical transport solution that is meant to adapt to the bandwidth demands of the network it is deployed in and ensure secure transfer of data across the network. Thus, the TOE is a network device composed of hardware and software.

3.1 TOE Evaluated Configuration

The TOE is comprised of both software (release 22.2.2) and hardware. The hardware is comprised of the following:

		FSP 3000R7 Series			
	PROPERTY	SH1HU	SH7HU	SH9HU	Acronym Definitions
Management Plane	Power	AC/DC/Mix	AC/DC/Mix	AC/DC/Mix	NCU-Network Control Unit
	Processor	NCU-3 (NXP QorIQ T-Series T1042E)	NCU-3 (NXP QorIQ T-Series T1042E)	NCU-3 (NXP QorIQ T-Series T1042E)	
	Local Console Connection	RJ45 Jack Serial Connector 1 USB Port	RJ45 Jack Serial Connector 1 USB Port	RJ45 Jack Serial Connector 1 USB Port	
	Management Network Connection	3 RJ45 Ethernet	3 RJ45 Ethernet	3 RJ45 Ethernet	
	Size	1 rack unit	7 rack units	9 rack units	
	Module Slots	2	16	16	
	Commons	FAN/1HU, PSU/1HU-AC, PSU/1HU-DC	FAN/Plug-in, PSU/7HU-AC, PSU/7HU-DC	CEM/9HU, FAN/9HU, PSU/9HU-AC, PSU/9HU-DC	PSU/HU-Power Supply Unit/Housing Unit CEM-Common Equipment Module

Table 2 – FSP 3000R7 Model Properties

The following table lists components and applications that are used in the Operational Environment for the TOE's evaluated configuration. These components and the functionality they provide are outside the scope of evaluation testing but are needed to support the tested functionality of the TOE.

Component	Definition
Terminal	A terminal is a device that handles the input and display of data when connected to an appliance's serial port. The TOE's CLI can also be accessed locally with a physical connection to the TOE using the Electrical connector type RJ45 or the serial port and must use a VT100 terminal emulator that is compatible with serial communications. Synonymous with the term local console. This OE component is required to support interface E1 as defined in Figure 1 above.
Remote Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. For the TOE to be managed remotely the management workstation is required to have:

Component	Definition
	• Supported browser to access the TOE's Web GUI • SSHv2 client installed to access the TOE's CLI The TOE acts as a server for all protocols. TCP communications from the Remote Management Workstation to the TOE is secured using: • SSH for remote access to the CLI • HTTPS for remote access to the Web GUI This OE component is required to support interfaces E2 & E3 as defined in Figure 1 above.
Audit Server	The TOE acts as a TLS client when connected to an Audit Server to send the audit records for remote storage. This OE component is required to support interface E4 as defined in Figure 1 above to send copies of audit data to be stored in a remote location for data redundancy purposes.
Certificate Authority (CA) Server	A server that acts as a trusted issuer of digital certificates and distributes a CRL that identifies revoked certificates. This OE component is required to support interface E5 as defined in Figure 1 above.
NTP Server	The TOE can connect to a NTP Server to maintain accurate timestamps for the TOE and the audit records generated. This OE component is required to support interface E6 as defined in Figure 1 above.
OTH or WDM Network	The OTH or WDM Network represents the optical transport hierarchy and wavelength division multiplexing components. Figure 1 identifies these interfaces as a single interface. The interface to the managed OTH or WDM Network is a separate connection to the enterprise Operational Environment the TOE is managing. There are no SFR's to address the TOE's management of the OTH or WDM Network. Therefore, interface E7 to these components is out of scope for the NDcPP and the present evaluation. This interface and components are included for completeness only.

4 Security Policy

This section summarizes the security functionality of the TOE.

4.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. The TOE stores audit logs locally and will free up audit storage space by deleting archived files in a First in First out (FIFO) fashion. The Security Administrator can configure the forwarding of events to an external Audit Server. In the evaluated configuration, the audit data is securely transmitted to the Audit Server using a TLS v1.2 communication channel.

4.2 Cryptographic Support

The TOE provides cryptography in support of SSH and TLS (v1.2) trusted communications. OpenSSL is used for all TLS and SSH communications. The TOE immediately destroys keys when no longer used. The following table identifies the cryptographic services:

SFR	OpenSSL Implementation	CAVP
FCS_CKM.1	ECC schemes using NIST curves P-384 following FIPS PUB 186-4	#**A4284**
	FFC using safe-prime groups NIST Special Publication 800-56A Revision 3 and RFC 3526.	N/A
FCS_CKM.2	Elliptic curve-based key establishment per NIST Special Publication 800-56A Revision 3	#**A4284**
	FFC using safe-prime groups NIST Special Publication 800-56A Revision 3 and RFC 3526.	N/A
FCS_COP.1/DataEncryption	AES CTR 256 bits AES GCM 256 bits	#**A4284**
FCS_COP.1/SigGen	ECDSA FIPS 186-4 Signature Services 384 bits	#**A4284**
FCS_COP.1/Hash	SHA-384 and SHA-512	#**A4284**
FCS_COP.1/KeyedHash	HMAC-384	#**A4284**
FCS_RBG_EXT.1	CTR DRBG (AES-256)	#**A4284**

4.3 Identification and Authentication

The TOE enforces the use of X.509 certificates to support authentication for all TLS connections. The TOE provides a password-based authentication mechanism for users to access the local CLI, remote CLI and Web GUI. The TSF will lock a user's account from remote access after a configurable number of failed login attempts has been reached. Feedback from password entry is always obscured during local authentication. The only function available to an unauthenticated user is the ability to acknowledge a warning banner.

4.4 Security Management

The TOE uses role-based access control to prevent unauthorized management of and access to TSF data. The TOE maintains the role of Security Administrator which can administer the TOE locally and remotely.

.

4.5 Protection of the TSF

The TOE ensures the security and integrity of all data that is stored locally and accessed remotely. Passwords are not stored in plaintext. A Security Administrator can query the currently executing version of the TOE software and is required to manually initiate the update process. Prior to installation, the TOE automatically verifies the X.509 certificate used to sign the software update. In the evaluation configuration, if the certificate is found to be invalid for any reason or is missing, the update is not installed. The TOE implements a self-testing mechanism that is automatically executed during the initial start-up to verify the correct operation of the TOE and cryptographic functions. The TOE provides its own time either via its administratively configurable internal clock or via a connection to an NTP Server.

4.6 TOE Access

The TOE displays a configurable warning banner prior to user authentication. Users can terminate their own interactive session. Local and remote sessions are automatically terminated after the administrator configured inactivity time limit is reached.

4.7 Trusted Path/Channels

Users can access the CLI for administration functions locally via a physical connection to the TOE or remotely via a SSH connection where the TOE acts as a SSH Server. Users can also access the Web GUI for remote administrative functionality via a HTTPS connection where the TOE acts as a HTTPS/TLS server.

The TOE acts as a TLS client to initiate the secure channel to an external Audit Server.

5 Assumptions and Clarification of Scope

5.1 Assumptions

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

- *collaborative Protection Profile for Network Devices*, v2.2e, 23 March 2020 (NDcPP22e)

That information has not been reproduced here and the NDcPP22e should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in NDcPP22e as described for this TOE in the ST. 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 in accordance with the evaluation activities specified in NDcPP22e and performed by the Evaluation team.
- This evaluation covers only the specific software version identified in this document and referenced in the *Adtran's FSP 3000R7 Network Element r22.2.2 Security Target v1.0*, dated January 10, 2024, and not any earlier or later versions released or in process.
- Apart from the Admin Guides identified in Section 6, additional customer documentation for the specific software version and platform versions was not included in the scope of the evaluation and, therefore, should not be relied upon when configuring or operating the device as evaluated.
- 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

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

- *Adtran's FSP 3000R7 Network Element r22.2.2 Supplemental Administrative Guidance for Common Criteria*, v1.0, January 12, 2024
- *Secure System Configuration Guide, Fiber Service Platform 3000R7,* Product Release 22.2
- *Network Element Director, Fiber Service Platform 3000R7,* Product Release 22.2
- *Installation and Commissioning Manual Fiber Service Platform 3000R7*, Product Release 22.2

To use the product in the evaluated configuration, the product must be installed and configured as specified in *Adtran's FSP 3000R7 Network Element r22.2.2 Supplemental Administrative Guidance for Common Criteria*. This document provides references to other documentation for specific steps to place the TOE into its the evaluated configuration and these documents are provided on the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the Evaluation team. It is derived from information contained in the *Adtran's FSP 3000R7 Network Element r22.2.2 Assurance Activities Report* v1.0, dated March 17, 2024 (AAR).

7.1 Test Configuration

The Evaluation team configured the TOE for testing according to the *Adtran's FSP 3000R7 Network Element r22.2.2 Supplemental Administrative Guidance for Common Criteria*, Version 1.0 (AGD) document. The Evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces. The Evaluation team conducted testing in the Booz Allen CCTL facility on an isolated network.

The TOE platforms were configured to communicate with the following environment components as demonstrated in Figure 1:

- Syslog server
- NTP Server (5)
- OCSP Responder (CRL Distribution/Certificate Authority)
- Workstations for local and remote administration, MITM testing, and penetration testing.

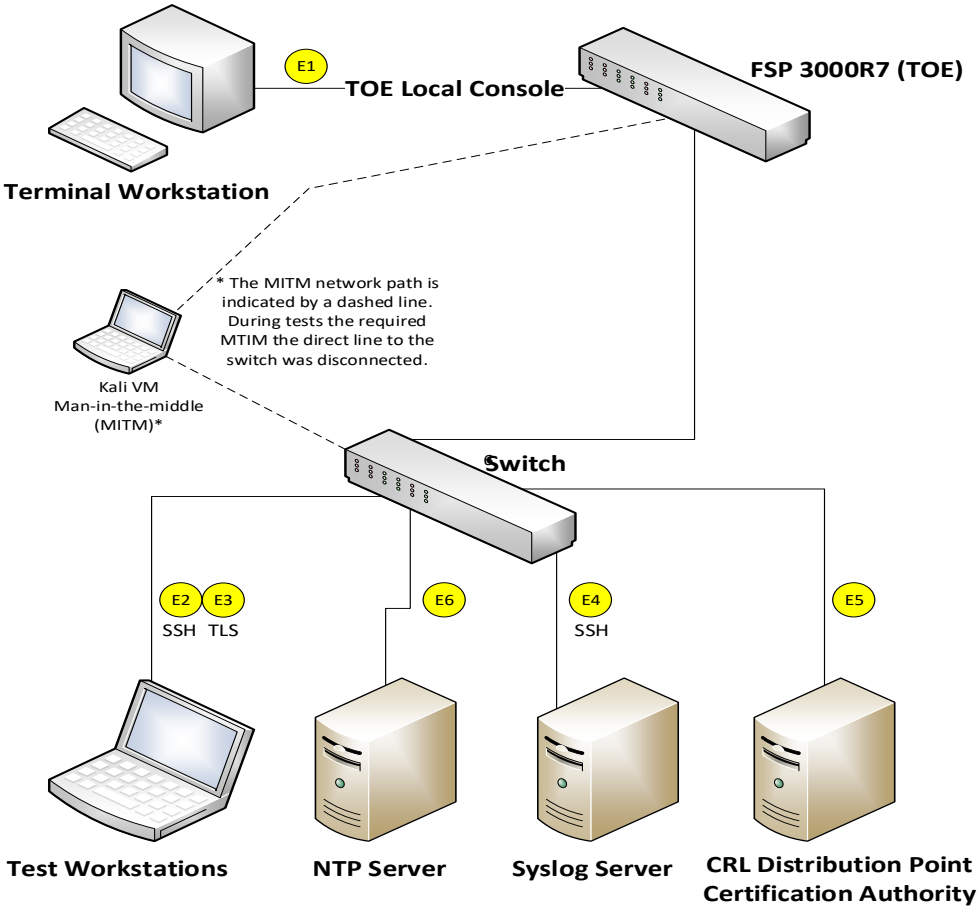

Figure 1 - Test Configuration

7.2 Developer Testing

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

7.3 Evaluation Team Independent Testing

The Evaluation team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDcPP22e.

Security functional requirements were determined to be appropriate to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The Evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

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 ETR and Detailed Test Report (DTR). The reader of this document can assume that all Evaluation 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 and the specific evaluation activities specified in the NDcPP22e Supporting Document. The Evaluation determined the TOE to be Part 2 extended and Part 3 conformant. The Validation team reviewed the work of the Evaluation team and agreed with their practices and findings.

8.1 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 Adtran's FSP3000R7 product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the Evaluation team performed an assessment of the Evaluation Activities specified in the NDcPP Supporting Documents to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

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 the Development (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed Protection Profile for design evidence. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluator performed the Evaluation Activities related to the examination of the information contained in the TOE Summary Specification.

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.

8.3 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the Evaluation team performed the Evaluation Activities specified in the NDcPP Supporting Document related to the examination of the information contained in the operational guidance documents.

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.

8.4 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 appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

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.

8.5 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 NDcPP Supporting Documents and recorded the results in a DTR, summarized in the ETR and sanitized for non-proprietary consumption in the AAR.

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.

8.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is documented in the proprietary *Adtran's FSP 3000R7 Network Element r22.2.2 Vulnerability Analysis*, Version 1.1, March 16, 2024, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on March 16, 2024, did not uncover any residual vulnerability.

The following keywords (version information used for refining results) were used during the public search:

Keyword	Description
ADVA	This is a generic term for searching for known vulnerabilities produced by the acquired company as a whole.
Adtran	This is a generic term for searching for known vulnerabilities produced by the new acquiring company as a whole.
FSP3000/FSP 3000/FSP-3000	This is a generic term for searching for known vulnerabilities for the specific product.
SH1HU, SH7HU, SH9HU	These are the models for searching for known vulnerabilities for the specific product.
NCU-3/NCU3/NCU 3	This is a generic term searching for known vulnerabilities for the underlying operating system.
FSP Network Element	This is a generic term searching for known vulnerabilities for the underlying operating system.
Network Control Unit	This is a generic term searching for known vulnerabilities for the underlying operating system.
Libraries	

Keyword	Description
Provided in a separate proprietary spreadsheet.	See Spreadsheet
Hardware	
T1042 (NXP QorIQ T-Series T1042E)	This is a generic term searching for known vulnerabilities for the TOE's underlying host processor.

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability. The following public vulnerability sources were searched:

- NIST National Vulnerabilities: https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security http://nessus.org/plugins/index.php?view=search
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

Upon the completion of the vulnerability analysis research, the Evaluation team identified several generic vulnerabilities upon which to build a test suite. The Evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

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 Evaluation Activities in the NDcPP22e Supporting Document, 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 *Adtran's FSP 3000R7 Network Element r22.2.2 Supplemental Administrative Guidance for Common Criteria Version 1.0* document. As noted in Section 6, consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated. No versions of the TOE and software, either earlier or later, were evaluated. Any additional customer documentation, not listed in Section 6, provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore, should not be relied upon to configure or operate the TOE as evaluated.

Administrators should take note of the fact that when the product is configured to offload audit files to an audit logging server, if that communications link is interrupted, the audit files generated during the time of the interruption will be captured locally. However, upon resumption of the connectivity, the offload begins with the reconnection and will NOT send those audit files generated during the outage. It will be necessary for the administrator to take steps to offload those files, or they will be overwritten when the audit log is full.

The Validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

10 Annexes

Not applicable

11 Security Target

The security target for this product's evaluation is *Adtran's FSP 3000R7 Network Element r22.2.2 Security Target v1.0*, dated January 10, 2024.

12 List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certificate Authority
CAVP	Cryptographic Algorithm Verification Program
CC	Common Criteria
CLI	Command-Line Interface
cPP	collaborative Protection Profile
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSP	Content Security Policy
DRBG	Deterministic Random Bit Generator
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
I&A	Identity and Access
IP	Internet Protocol
MAC	Message Authentication Code
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OS	Operating System
OTH	Optical Transport Hierarchy
PP	Protection Profile
RAM	Random Access Memory
RBG	Random Bit Generator
RNG	Random Number Generator
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell
ST	Security Target
SVR	Server
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
WDM	Wavelength-Division Multiplexer

13 Glossary

Term	Definition
Administrator or 'Admin'	A user who is assigned the 'Admin' role on the TOE and has the ability to manage the TSF. Synonymous with Security Administrator.
Credential	Data that establishes the identity of a user (e.g., a cryptographic key or password).
Operating System (OS)	Software that manages hardware resources and provides services for applications.
Platform	A platform can be an operating system, hardware environment, a software-based execution environment, or some combination of these. These types of platforms may also run atop other platforms.
Security Administrator	An authorized administrator role that is authorized to manage the TOE and its data. This TOE defines three separate user roles, but only the most privileged role (Admin) is authorized to manage the TOE's security functionality and is therefore considered to be the Security Administrator for the TOE.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application a Security Administrator uses to manage it (SSH client, terminal client, etc.).
User	In a CC context, any individual who has the ability to access the TOE functions or data.

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*, v2.2E, 23-March-2020
6. *Adtran's FSP 3000R7 Network Element r22.2.2 Security Target,* v1.0, dated January 10, 2024
7. *Adtran's FSP 3000R7 Network Element r22.2.2 Supplemental Administrative Guidance for Common Criteria*, v1.0, dated January 12, 2024
8. *Secure System Configuration Guide, Fiber Service Platform 3000R7,* Product Release 22.2
9. *Network Element Director, Fiber Service Platform 3000R7,* Product Release 22.2
10. *Installation and Commissioning Manual Fiber Service Platform 3000R7*, Product Release 22.2
11. *Adtran's FSP 3000R7 Network Element r22.2.2 Assurance Activities Report* Version 1.0 dated March 17, 2024
12. *Adtran's FSP 3000R7 Network Element r22.2.2 Evaluation Technical Report*, Version 1.0, dated March 17, 2024
13. *Adtran's FSP 3000R7 Network Element r22.2.2 Vulnerability Analysis*, Version 1.1, dated March 16, 2024
14. *Adtran's FSP 3000R7 Network Element r22.2.2 Test Plan*, Version 1.0, February 16, 2024