ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Forescout v8.4.1

Forescout v8.4.1

Maintenance Report Number: CCEVS-VR-VID11279-2023

Date of Activity: May 2, 2023

References

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Forescout v8.4.1 Security Target, ST Version 2.1, 27 February March 2023
- collaborative Protection Profile for Network Devices Version 2.2e, 27 March 2020

Assurance Continuity Maintenance Report

Forescout Technologies, Inc. submitted an Impact Analysis Report (IAR), for the "Forescout v8.4.1" network device to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 22 March 2023. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The IAR was prepared by the Booz Allen Hamilton Cyber Assurance Testing Laboratory on behalf of Forescout. The evaluation evidence submitted for consideration consisted of the Security Target (ST), updated Guidance Documentation described further in the table below, the Impact Analysis Report (IAR), and release notes.

Documentation updated

Evidence Identification	Effect on Evidence/ Description of Changes
Impact Analysis Report Forescout Version 8.4.1 Impact Analysis Report (IAR) Version 1.0, May 2, 2023	**Evaluation Evidence:** New – summarized the old TOE, new TOE, provides an explanation of the changes and rationale of why the changes are sufficiently minor to claim the original evaluation's work still applies sufficiently.
Security Target Forescout v8.4.1 Security Target, ST Version 2.1, 27 February 2023	**The Security Target** – the Security Target document was updated to be applicable to the updated versions of the TOE for version 8.4.1: o v8.4.1 Common Criteria Security Target v2.1 dated February 27, 2023. Updates include: • Identification of the Changed TOE version (8.4.1) • Security Target dates and versioning (v2.1, February 27. 2023) • The excluded from the evaluated configuration list (added RADIUS, Forescout Cloud services, REST Admin API) • The Technical Decision table: o TD0638 TOE supports the key generation for RSA which is the same claimed for FTP_ITC and FTP_TRP. o TD0639 does not claim NTP o TD670 does not claim mutual auth
Guidance Forescout Continuum v8.4.1 Supplemental Administrative Guidance v1.1 dated February 27, 2023.	**The Guidance Document** – The guidance document was updated to be applicable to the updated versions of the TOE for versions 8.4.1: o Forescout Continuum v8.4.1 Supplemental Administrative Guidance v1.1 dated February 27, 2023. • Identification of the Changed TOE version (8.4.1) • Update of document dates and versioning (v1.1 dated February 27, 2023) • Update of references to Changed TOE Security Target and other guidance documentation ▪ NOTE: The TOE has a new selectable audit feature that was not tested as part of the evaluated configuration. In order to satisfy all of the audit requirements defined in the NDcPP all audit records with all severity levels must be generated. Therefore, this feature cannot be used in the evaluated configuration. • Update guidance to provide steps to ensure the REST Admin API plugin is disabled.
Release Notes	o The release notes were created for each patch between the Validated TOE (version 8.3.0) and the Changed TOE (version

	8.4.1). They contain a listing of the new features implemented and bug fixes provided by these patches.

Changes to the TOE

Each of the changes to "Forescout v8.4.1" was analyzed to determine whether it fell into the categorization of "Major Changes" or "Minor Changes". The conclusion was that all of the changes were minor and had either minor or no impact on the evaluated product.

New Features

The IAR New Features Section contains a table listing the new features that have been added for all releases between the Validated TOE and the Changed TOE along with a brief description of each feature. The New Features table lists 38 new features. Of these, 21 have no impact to the Security Target, the ADV_FSP functional specification, ATE test procedures, or the AGD guidance documentation. There are 15 new features that caused exclusion list in the Security Target to be updated. There are 3 new features that caused the AGD to be updated; one of these also has a feature excluded in the ST.

New Features with no impact on the ST, ADV, ATE, or AGD

1. Forescout Platform 8.4 Pre-Upgrade Verifier
2. Forescout Platform 8.4 Smartcard Group
3. Forescout Platform 8.4 Endpoints Behind NAT/SASE
4. Forescout Platform 8.4 fstool Command: unlock_console_user
5. Forescout Platform 8.4 eyeExtend Connect Version
6. Core Extensions Module 1.4 Active Probing 1.0.1: New Active Probing Plugin
7. Core Extensions Module 1.4 CEF 3.0: Include Syslog Message Header
8. Endpoint Module 1.4 HPS Inspection Engine 11.3
9. Endpoint Module 1.4 Linux 1.7: Additional Requirements
10. Network Module 1.4 Centralized Network Controller 1.4
11. Network Module 1.4 Switch Plugin 8.16: New Switch API for Switch Definition and Management
12. Network Module 1.4 Switch Plugin 8.16: Switch Health Alerts
13. Continuum Platform 8.4.1 Virtual Machine Resources Check
14. Core Extensions Module 1.4.1 Active Probing Plugin 2.0: New Host Properties
15. Core Extensions Module 1.4.1 Active Probing Plugin 2.0: Deprecated Host Properties
16. Endpoint Module 1.4.1 OS X Plugin 2.5.1
17. Network Module 1.4.1 Switch Plugin 8.16.3 Plugin Adds Management of Vendor Switches: DNI
18. Network Module 1.4.1 Switch Plugin 8.16.3 Plugin Adds Management of Vendor Switches: Accton
19. Network Module 1.4.1 Switch Plugin 8.16.3 Plugin Adds Management of Vendor Switches: QuantaMesh
20. Network Controller Plugin 1.2.1: Support for Additional Vendors and Solutions
21. Network Controller Plugin 1.2.1: Assign Cisco ACI Controllers to VLAN

New Features that required an update to the exclusion list in the Security Target

1. Forescout Platform 8.4 Risk Scoring Service
2. Authentication Module 1.4 RADIUS 4.7: Enable SASL Encryption for LDAP Bindings
3. Authentication Module 1.4 RADIUS 4.7: MAC Address Repository (MAR) Expiration and Removal
4. Authentication Module 1.4 RADIUS 4.7: FreeRADIUS Version Upgraded
5. Core Extensions Module 1.4 Admin API 1.0: New Admin API
6. Core Extensions Module 1.4 Device Classification Engine 1.6
7. Hybrid Cloud Module 2.3
8. Cloud Tools Module 1.0.1

9. Continuum Platform 8.4.1 Forescout Cloud Features Onboarding
10. Continuum Platform 8.4.1 Forescout Cloud Features Multifactor Risk Scoring
11. Continuum Platform 8.4.1 Forescout Cloud Features eyeSegment
12. Continuum Platform 8.4.1 Forescout Cloud Features Classification Feedback Dialog
13. Authentication Module 1.4.1 RADIUS Plugin 4.7.2: Addition of Endpoint Attribute for Pre-Admission Authorization Rules
14. Core Extensions Module 1.4.1 Cloud Uploader 1.3.1: Cloud Connectivity Test Results Provide Additional Information
15. Hybrid Cloud Module 2.3.1

New Features requiring updates to the Guidance documentation

1. Core Extensions Module 1.4 Admin API 1.0: New Admin API (feature also added to the exclusion list in the ST)
2. Forescout Continuum Platform 8.4.1 Configure Audit Trail Logging
3. Continuum Platform 8.4.1 CLI User Not Subject to Lockout

The new features were found to have a no impact or only minor security impact due to enhancements in areas of validated functionality. For new features with minor security impacts, the vendor has demonstrated that these new features are properly implemented by providing evidence of regression testing to demonstrate that these new features do not adversely affect the behavior of the TSF. There are no changes that modify the implementation of SFRs, remove the enforcement of existing SFRs, or force the addition of any security-relevant functionality or interfaces.

In version 8.4.1, Forescout started rebranding the product to be known as the Forescout Continuum Platform. The rebranding will be complete with the next major release 9.0. Therefore, for this assurance maintenance request, the TOE will still be considered Forescout v8.4.1. The name change alone presents no technical/security functionality changes to the product.

Bug Fixes

The IAR contains the list of bug fixes made between the Validated TOE and the Changed TOE, with a brief description of the nature of the fix. There are 26 sets of these bug fixes which are summarized below. The vendor has demonstrated that these bug fixes are properly implemented by providing evidence of regression testing to demonstrate that these bug fixes will not have adversely affected the behavior of the TSF. None of the bug fixes impacted the ST, ADV, ATE or AGD.

Bug Fix	Description
CA-29082, OF-611	Forescout Platform 8.4 Fixed Issues
CA-28784, OF-610	Forescout Platform 8.4 Fixed Issues
VMW-970	Forescout Platform 8.4 Fixed Issues
DOT-4616	Authentication Module 1.4 Fixed Issues
DCE-532	Core Extensions Module 1.4
TS-418	Core Extensions Module 1.4
VMW-970	Hybrid Cloud Module 2.3
ESC-7499	Cloud Tools Module 1.0.1
PM-14922	Continuum Platform 8.4.1
CA-29991	Continuum Platform 8.4.1
CA-29965	Continuum Platform 8.4.1
CA-29746	Continuum Platform 8.4.1
CA-29900	Continuum Platform 8.4.1
CA-29749	Continuum Platform 8.4.1

CA-29735	Continuum Platform 8.4.1
CA-29747	Continuum Platform 8.4.1
DOT-4674, DOT-4675, DOT-4717	Authentication Module 1.4.1
DOT-4712/DOT-4716	Authentication Module 1.4.1
DOT-4713/DOT-4715	Authentication Module 1.4.1
UD-2166	Authentication Module 1.4.1
DSH-632	Core Extensions Module 1.4.1
DNQ-79	Core Extensions Module 1.4.1
TS-450	Core Extensions Module 1.4.1
EPM-328	Endpoint Module 1.4.1
VMW-980	Hybrid Cloud Module 2.3.1
SCC-689, SCC-691, SW-6729, SW-6761	Network Module 1.4.1

TOE Environment

There are no updates to hardware or other operational environment components identifies to analyze. Therefore, it was determined that they were consistent with the validated results from the previous evaluation.

Regression Testing

Forescout performs continuous testing on Forescout Platform code with testing cycles occurring multiple times a day and ensures that each piece of updated code is tested several times before a new image is released. Any time a bug is fixed, or a new feature is implemented in the Forescout platform, the new code is unit tested to ensure that it operates correctly. The code will then be merged with the base code where Forescout's Quality Assurance System performs a full suite of unit tests and operational tests to verify that the code changes were properly implemented and do not impact any of Forescout Platform's other functionality.

Included in the Quality Assurance's operational test suite are targeted test cases that were performed during the Common Criteria certification of Forescout Platform version 8.3.0 (Validated TOE). Once Forescout is ready to release a new software image, Forescout will create a build of the software for the release which is also tested using Forescout's Quality Assurance System. The unit tests and operational tests that comprise the Quality Assurance System are maintained by Forescout's developers and Quality Assurance team to ensure that tests are updated to test the latest code.

Forescout performed regression testing on Forescout Platform 8.4.1 (Changed TOE) and determined that the behavior of the TSF remained consistent with the testing during the original evaluation.

Cryptographic Support: NIST CAVP Certificates

There are no changes to the cryptographic support. Both the evaluated TOE and the changed the TOE implement the same two different cryptographic libraries: OpenSSL and Bouncy Castle. Both libraries include algorithms that are certified under the following consolidated CAVP certificates:

a) OpenSSL FIPS library under CAVP Certificate # C1887 and A1941

b) BC-FJA (Bouncy Castle FIPS Java API) Software Version 1.0.2 under CAVP Certificate # C1888 and A1959

Vulnerability Analysis

The lab defined keywords to perform a public search for vulnerabilities. The keywords are defined based on the vendor's name, product (TOEs) name, general technology product terms, and libraries compiled with the TOE. The previous evaluation public searches were updated on October 12, 2022, and on February 27, 2023. Therefore, the results did not duplicate what was previously reported and approved but focused on new items found since that point. A public search for vulnerabilities that might affect the TOE was performed on May 2, 2023. All applicable findings must be resolved to pass.

The following public sources were searched during this analysis:

a) NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
b) Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
c) US-CERT: http://www.kb.cert.org/vuls/html/search
d) Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
e) Offensive Security Exploit Database: https://www.exploit-db.com/
f) Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

The following keywords were used individually and as part of various permutations and combinations to search for vulnerabilities identified in the public domain:

Keyword	Description
Forescout	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
CounterACT	This is a generic term for searching for known vulnerabilities for the specific product. NOTE: The TOE is no longer referred to as CounterACT, however, we still included this in our search because the product name change was recent.
CentOS 7.5	This is a term for searching for known vulnerabilities for the underlying OS. A specific version was not included in the search because this version may be within a range of vulnerable operating system versions and not listed separately. Bearing in mind that this is a locked operating system that has been enhanced by the vendor who is not using the full functionality of the OS.
Model/nomenclature CEM CT-R, CT-100, CT-1000, CT-2000, CT-4000, CT-10000, CEM-5, CEM-10, CEM-25, CEM-50, CEM-100, CEM-150, CEM-200, 4130, 5110, 5120, 5140, and 5160.	Specific models search / nomenclature search
Generic Terminology	
Central Enterprise Manager	Generic term
Libraries	
OpenSSL (1.0.2k build 23)	This is a term for searching for known vulnerabilities for the underlying cryptographic software utilized by the TOE. A specific version was not included in the search because this version may be within a range of vulnerable operating system versions and not listed separately. However, the version was used to further filter findings.

OpenSSH 7.4p1-22	This is a term for searching for known vulnerabilities for the OpenSSH server utilized by the TOE. A specific version was not included in the search because this version may be within a range of vulnerable operating system versions and not listed separately. However, the version was used to further filter findings.
BC-FJA 1.0.2 (Bouncy Castle)	A specific version was not included in the search because this version may be within a range of vulnerable Bouncy Castle versions and not listed separately. However, the version was used to further filter findings.
OpenJDK 1.8.0_282 (8u282 alternative)	A specific version was not included in the search because this version may be within a range of vulnerable Java versions and not listed separately. However, the version was used to further filter findings.
PostgreSQL (Postgres) 13.1	A specific version was not included in the search because this version may be within a range of vulnerable Java versions and not listed separately. However, the version was used to further filter findings.
NMAP 7.91 and 5.21	A specific version was not included in the search because this version may be within a range of vulnerable Java versions and not listed separately. However, the versions were used to further filter findings. Both versions were part of the filtered search.
Hardware	
Intel Celeron J1900 (Bay Trail)	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites
Intel Xeon E5 2609 v3 (Haswell)	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites
Intel Xeon E5 2620 v3 (Haswell)	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites
Intel Xeon E5 2640 v3 (Haswell)	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites
Intel Xeon E5 2650 v3 (Haswell)	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites
Xeon Silver 4110 (Skylake)	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites
Xeon Silver 4114 (Skylake)	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites
Xeon Gold 5118 (Skylake)	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites
Xeon Gold 6132 (Skylake)	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites
Gen 8 Intel® Core™ i5-8500T (Coffee Lake)	Terms used in the advanced searches for NVD and CVE details websites. Generic terms used in various combinations for additional websites

There were no open or unpatched known vulnerabilities to the TOE, nor the libraries used by the TOE, as a result of the public search. Therefore, there are currently no publicly known vulnerability issues that could affect the security posture of a deployed TOE.

The validators confirmed that the vendor assessment determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

In summary, no vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE.

Conclusion

As documented in the IAR, there has been added functionalities and bug fixes between the Validated TOE (Forescout v8.3) to the Changed TOE (Forescout v8.4.1). A few of these updates improved the product's functionality related to the TSF by addressing security vulnerabilities, increasing performance, and addressing bugs that caused usability issues. However, most of these updates addressed functionality that was outside the scope of the evaluated configuration. The development evidence (Security Target and Supplemental Administrative Guidance) for the Validated TOE received minor updates to address the Changed TOE to include product and document version updates.

These new features and bug fixes did not impact the ability of the TOE to continue enforcing the security requirements as described by the Validated TOE's Security Target. Furthermore, the methods used to perform functions on the Validated TOE are still available to be used in the Changed TOE, since all updates made to the Changed TOE were done to allow for backwards compatibility to already configured SailPoint IdentityIQ instances. This was also verified through the completion of the regression testing that confirmed the functionality still operated as expected.

Based upon the findings in the IAR and the reasoning provided above in this document, it has been determined that the changes from the validated TOE (Forescout v8.3) to the Changed TOE (Forescout v8.4.1) are of "minor impact".

The overall impact is minor. This is based on the above rationale that new non-security relevant changes and the update of the TOE to Forescout v8.4.1 had no impact on the certified TOE.

In addition, a search for vulnerabilities identified none directly affecting the TOE

Therefore, CCEVS agrees that the original assurance is maintained for the product.