ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
Forescout v8.4.1.1-50 with CIUP v3.1.4

Maintenance Update of Forescout v8.4.1.1-50 with CIUP v3.1.4

Maintenance Report Number: CCEVS-VR-VID11279-2024

Date of Activity: 20 June 2024

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016.
- Forescout v8.4.1.1-50 with CIUP v3.1.4 Impact Analysis Report (IAR) Version 1.1, June 7, 2024.
- collaborative Protection Profile for Network Devices Version 2.2e.

Documentation Updated:

The following assurance evidence was affected by the release of the Forescout v8.4.1.1-50 with CIUP v3.1.4 and resulted in updated documentation:

- Security Target – The Security Target document below was updated to be applicable to the updated version of the TOE for v8.4.1.1-50 with CIUP v3.1.4:
    - Forescout v8.4.1.1-50 with CIUP v3.1.4 Common Criteria Security Target v2.3 dated June 7, 2024. Updates include:
        - Identification of the Changed TOE version (v8.4.1.1-50 with CIUP v3.1.4)
        - Security Target dates and versioning (v2.3, June 7, 2024)
        - Note added and version references updated to section 2.4 to address the addition of CIUP v3.1.4
        - The Technical Decision table:
            - TD0738 – The TD is about updating a link to the PP’s ‘allowed-with list’ (removed superseded TD0538). Updating a link location is not impactful to the product. No impact to the evaluation.
            - TD0790 – The TD changes the wording of the conditional test for FCS_TLSC_EXT.1.2(removed superseded TD0634). The TD did not

change the reasons for being conditional, and therefore, the conditions still do not apply to the TOE. Thus, the changes to a conditional test that is not applicable to the TOE, has no impact on the evaluation.

- TD0792 – This TD results in a small FIA_PMG_EXT.1 TSS Assurance Activity wording update. The TSS wording required no change as it was already compliant. No impact to the evaluation.
- TD0800 – The TD has to do with IPSEC SFRs (removed superseded TD0633). Product does not claim IPSEC. No impact to the evaluation.

- Guidance Document – The guidance document below was updated to be applicable to the updated version of the TOE for versions 8.4.1.1-50 with CIUP v3.1.4:
    - Forescout v8.4.1.1-50 with CIUP v3.1.4 Supplemental Administrative Guidance v1.3 dated June 7, 2024.
        - Identification of the Changed TOE version (v8.4.1.1-50 with CIUP v3.1.4)
        - Update of document dates and versioning (v1.3 dated June 7, 2024)

Assurance Continuity Maintenance Report:

Forescout Technologies, Inc-submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 22 April 2024. 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 2.0. 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 evaluation evidence consists of the Security Target, the Supplemental Administrative Guidance, and the Impact Analysis Report (IAR). The ST and guide document were updated, the IAR was new.

New Features

Forescout v8.4.1.1-50 with CIUP v3.1.4 does not contain any new features that have been added since Forescout v8.4.1 underwent the assurance maintenance process.

Bug Fixes

Forescout v8.4.1.1-50 with CIUP v3.1.4 contains bug fixes that have been added since Forescout v8.4.1 completed the previous assurance maintenance process on 5/3/2023. All bug fixes mentioned below were implemented to address published vulnerabilities and were judged to be minor.

Bug Fix	Description	Overall Impact
Apache Server	Apache Server has been upgraded to version 2.4.59 to address published vulnerabilities.	No Impact
Apache Tomcat	Apache Tomcat has been upgraded to version 8.5.99 to address published vulnerabilities.	No Impact
Jackson Databind	Jackson Databind has been upgraded to version 2.16.0 to address published vulnerabilities.	No Impact
OpenSSL	OpenSSL has been upgraded to version 1.0.2k-26 to address published vulnerabilities.	No impact
Zlib	Zlib has been upgraded to version 1.2.7-21 to address published vulnerabilities.	No impact
Python2	Python2 has been upgraded to version 2.7.5-94 to address published vulnerabilities.	No impact
BIND	BIND has been upgraded to version 9.11.4-26.P2.el7_9.15 to address published vulnerabilities.	No impact
Grub2	Grub2 has been upgraded to version 2.02-0.87.0.2.el7.centos.11 to address published vulnerabilities.	No impact
OpenSSH	OpenSSH has been upgraded to version 7.4p1-23.el7_9.fs.1 to address published vulnerabilities.	No impact
LibXpm	LibXpm has been upgraded to version 3.5.12-2 to address published vulnerabilities.	No impact

TOE Environment

There are no updates to operational environment components identified. The TOE environment is consistent with the validated results from the previous evaluation.

Regression Testing

Forescout performs continuous testing on the Forescout product 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 product, 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 product's other functionality.

Forescout performed regression testing on Forescout v8.4.1.1-50 with CIUP v3.1.4 (Changed TOE) and determined that the behavior of the TSF remained consistent with the testing during the original evaluation.

NIST CAVP Certificates:

The updates made to the TOE have not changed the cryptographic modules algorithm implementation nor their tested operational environment, so there is no impact to the CAVP certificates.

Vulnerability Analysis:

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) U.S.-CERT: http://www.kb.cert.org/vuls/html/search
d) Tenable Network: www.tenable.com/plugins/search
e) Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
f) Offensive Security Exploit Database: https://www.exploit-db.com/
g) 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: The searches were performed on May 2, 2023, and again on June 4, 2024.

Forescout
CounterACT
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.
Generic Terminology
Central Enterprise Manager
Libraries
CentOS 7.5
OpenSSL (1.0.2k build 26)
OpenSSH 7.4p1-23
BC-FJA 1.0.2 (Bouncy Castle)
NMAP 7.91 and 5.21
PostgreSQL (Postgres) 13.1
OpenJDK 1.8.0_282 (8u282 alternative)
New Libraries
Gzip-1.5-11
Zlib 1.2.7-21
Apache HTTP Server 2.4.59
Apache Tomcat 8.5.99
Jackson-databind 2.16.0
rpm-4.11.3-48
rpm-build-libs-4.11.3-48
rpm-libs-4.11.3-48
rpm-python-4.11.3-48
audit-libs-2.8.5-4
libcap-ng-0.7.5-4
libssh2-1.8.0-4
nss-util-3.79.0-1
nss-softokn-3.79.0-4
nss-3.79.0-5
nss-softokn-freebl-3.79.0-4
nss-tools-3.79.0-5
nss-sysinit-3.79.0-5
kpartx-0.4.9-136
libXpm-3.5.12-2
grub2-2.02-0.87.0.2 .el7.centos.11
grub2-common-2.02-0.87.0.2
grub2-efi-x64-2.02-0.87.0.2
grub2-pc-2.02-0.87.0.2
grub2-pc-modules-2.02-0.87.0.2
grub2-tools-2.02-0.87.0.2
grub2-tools-extra-2.02-0.87.0.2
grub2-tools-minimal-2.02-0.87.0.2
python-2.7.5-94
python-libs-2.7.5-94
open-vm-tools-11.0.5-3
bind-9.11.4-26.P2.el7_9.15
bind-chroot-9.11.4-26.P2
bind-libs-9.11.4-26.P2
bind-license-9.11.4-26.P2
bind-utils-9.11.4-26.P2
bind-libs-lite-9.11.4-26.P2
bind-export-libs-9.11.4-26.P2
Hardware
Intel Celeron J1900 (Bay Trail)
Intel Xeon E5 2609 v3 (Haswell)
Intel Xeon E5 2620 v3 (Haswell)
Intel Xeon E5 2640 v3 (Haswell)
Intel Xeon E5 2650 v3 (Haswe ll)
Xeon Silver 4110 (Skylake)
Xeon Silver 4114 (Skylake)
Xeon Gold 5118 (Skylake)
Xeon Gold 6132 (Skylake)
Gen 8 Intel® Core™ i5-8500T (Coffee Lake)

There were no open or unpatched known vulnerabilities discovered in the product, or the libraries used. Therefore, there are currently no publicly known vulnerability issues that could affect the security posture of a deployed product.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. No functionality, as defined in the SFRs, was impacted, and none of the bug and vulnerability updates affected the security functionality or the SFRs identified in the Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.