CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, and PA-5000 Series Next-Generation Firewall running PAN-OS 5.0.11

Maintenance Report Number: CCEVS-VR-VID10392-2014

EAL: 4 + ALC_FLR.2 + ATE_DPT.3

Date of Activity: 9 September 2014

References:

CCIMB-2004-02-009 Assurance Continuity: CCRA Requirements, Version 1.0, February 2004

Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 2, September 8, 2008

“Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, and PA-5000 Series Next-Generation Firewall running PAN-OS 5.0.11 Impact Analysis Report” Revision 2.0, September 9, 2014.

Documentation Updated:

Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, and PA-5000 Series Next-Generation Firewall running PAN-OS 5.0.11 Security Target Version 2.1, September 9, 2014

Common Criteria Evaluation Configuration Guide for Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, and PA-5000 Series Next-Generation Firewall running PAN-OS 5.0, Version 2.0, March 6, 2014

Introduction:

On March 7, 2014, Leidos Common Criteria Testing Laboratory, on behalf of Palo Alto Networks, submitted an Impact Analysis Report (IAR) to CCEVS for approval. 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", 8 September 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes, and the security impact of the changes.

Changes to TOE:

Palo Alto Networks has added support for 3 new appliance models, revised the firmware OS in their hardware appliances and revised the User Identification Agent software.

The following is a summary of the differences from the previously evaluated product:

1. Palo Alto Networks has revised the firmware OS in their hardware appliances from PAN-OS v4.0.12-h2 to PAN-OS 4.1 and again from PAN-OS 4.1 to PAN-OS 5.0.11.
2. The User Identification Agent software has been revised from v3.1.2 to v5.0.6.
3. The following three appliance models were added to the TOE:
    a. PA-200
    b. PA-3020
    c. PA-3050
4. The functionality of the new models remains the same with prior models. The code base is common across all product series and the new models use processors in the same families and with the same software images. All models use a Cavium processor on the data plane. The PA-200 uses a Cavium processor on the management plane similar to the PA-500 and the PA-2000. The PA-3000 models use an Intel processor on the management plane. The PA-4000 and PA-5000 also use an Intel processor on the management plane. The primary differences with the added models relate to capacity, speed and performance and are not security relevant in the context of this evaluation.
5. As a result of the above hardware and firmware changes, all appliance models have been FIPS 140-2 validated with PAN-OS 5.0.11 and the new certificate numbers are included in the updated Security Target.

Analysis and Testing:

CCEVS concluded that the changes included in the IAR did not have greater security impact than was reported, and that it could be classified as minor. No major changes were required in the ST.

Vendor analysis showed that the specific changes made to the PAN-OS and to the UIA do not affect the security claims in the Palo Alto Networks Next-Generation Firewall Security Target. Updates to evaluation evidence deliverables were primarily to reflect the current product OS revision, but otherwise were not changed in regard to how any of the security claims are met. Each of the test cases described in the updated test evidence were validated with the current (revised) version of the PAN-OS and new test results were produced and found consistent with the previous test results. Finally, the Palo Alto security team searched the public domain for any new potential vulnerabilities that may have been identified since the evaluation completed, but didn't find any that might affect any of the security claims.

Conclusion:

The validation teams reviewed the changes and concurs that the changes are minor and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.