ASSURANCE CONTINUITY MAINTENANCE REPORT FOR CISCO Nexus 5000 with v5.2(1)N1(2a)

Maintenance Update of Cisco Nexus 5000 with v5.2(1)N1(2a)

Maintenance Report Number: CCEVS-VR-VID10384-2014

Date of Activity: 31 March 2014

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;

Impact Analysis Report Common Criteria Assurance Maintenance for Cisco Nexus 5000 with v5.2(1)N1(2a), VID:10384, Prepared by: Cisco Systems, Inc., version 1.1, August 2013.

Documentation Updated: (List all documentation updated)

- Cisco Nexus 5000 Series Switch Security Target, Revision 1.2, March 2013, was updated from the previous version with additions and changes to the TOE identification and TOE description sections to add new hardware models and to replace software versions.
- Nexus 5000 Series Switch Nexus 2000 Series Fabric Extender Cisco Secure ACS, Preparative Procedures and Operational User Guidance (Common Criteria Specific) was updated to version 1.2 to add hardware models and update software versions.
- The Configuration Management, Lifecycle and Delivery Procedures for Cisco Nexus 5000/2000 Series document was updated to version 1.3 to reflect the additional hardware models and updated software versions.

Assurance Continuity Maintenance Report:

Cisco Systems, Inc. submitted an Impact Analysis Report (IAR) to CCEVS for approval in August 2013. 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 as a result of the changes and the security impact of the changes.

Changes to TOE:

The TOE includes a series of switches and related components, i.e., the Cisco Nexus 5000 Series Switch with 2000 Series Fabric Extenders, running software NX-OS version 5.2(1)N1(2a), and Cisco Secure Access Control Server (ACS) version 5.2 Patch 10. The Security Target and guidance documentation were updated to add the following hardware models to the TOE, which are all functionally equivalent to the evaluated hardware models:

- 5596T (the vendor notes this model is similar to 5596UP, 5548P, and 5548UP, which were in the previous TOE),
- 2248TP-E (the vendor notes this model is similar to 2248TP, which was part of the previous TOE),
- 2232TM, and 2232TM-E (the vendor notes these models are similar to 2232PP, which was part of the previous TOE), and
- B22F, and B22HP (the vendor notes these are smaller form-factor versions of the larger 2200 series switches).

The hardware models added to the TOE are functionally equivalent to models that were part of the original certified TOE. All the hardware models run the same version of NX-OS software, and all security functionality is implemented in the software. The 5596T runs the same newer NX-OS software image as the previously-certified 5596UP.

The 2248TP-E, 2232TM, 2232TM-E, B22F, and B22HP Fabric Extenders all have their system images installed from the parent 5500 switch the same way the previous-certified hardware models do when they're joined to the TOE, and all the new models provide the same security functionality as the other certified models.

The additional hardware models do not provide any security functionality; all the security functionality is enforced in the NX-OS software, thus none of the hardware changes to the TOE have any security relevance. The hardware models differ in terms of throughput and connectivity options. For example: The "UP" models include built-in "unified ports" which can each be configured as either Gigabit Ethernet (or FCoE), or Fiber Channel. The built-in ports of the "P" models only support Gigabit Ethernet (or FCoE), but not Fiber Channel.

To demonstrate the claim that the added hardware models are functionally equivalent, Cisco tested the added hardware models using the same test-bed configuration as the certified TOE, but replaced older/slower models with newer/faster models. The validators examined the test results and found that the test results were consistent with the certified test results.

The Security Target and guidance documentation were also updated to replace the previous software versions with updated software versions NX-OS 5.2(1)N1(2a) and ACS version 5.2 Patch 10. The software update consisted primarily of documented bug fixes and did not result in any changes to the security functionality of the TOE as documented in the Security Target. No additional security functional requirements were added to the Security Target and there were no changes to the existing security functional requirements in the Security Target. The updated Security Target includes no changes to any security functional requirements or descriptions of TOE functionality. No additional functionality was added that impacted the security functions of the TOE.

In an examination of the bug fixes implemented, the validators found that the fixes were either unrelated to the original security functional requirements in the Security Target or the bug fixes ensured that the product works as claimed in the original security functional requirements. All of the fixes applied to the TOE software resulted in functionality that is consistent with the certified functionality. To support this claim, Cisco re-ran the full set of certified vendor test cases and confirmed that the test results were consistent with the certified test results.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found it to be minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.