CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Cisco Systems Routers (800, 1700, 1800, 2600XM, 2800, 3700, 3800, and 7200 running Cisco IOS Release 12.4(15)T10; 7300 and 7600 running Cisco IOS Release 12.2(18)SXF16) and a Cisco Secure Access Control Server version 4.1.2.12

Maintenance Report Number: CCEVS-VR-VID6014-2008a

Date of Activity: 11 December 2009

References: Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004;

Impact Analysis Report for Common Criteria Assurance Maintenance Update of Cisco Systems Routers IOS 12.2(18)SXF8 to 12.2(18)SXF16 and IOS 12.4(11)T2 to 12.4(15)T10, version 0.2, November 2009.

Documentation Updated:

- Cisco Systems Routers EAL3 Security Target, Version 1.8, part number OL- 15545-01
- Installation and Configuration for Common Criteria EAL3 Evaluated Cisco IOS/AAA Routers
- Cisco AAA Configuration Items
- IOS / AAA Vulnerability, Misuse and Strength of Function EAL 3

Assurance Continuity Maintenance Report:

The vendor for the Cisco Systems Routers 800, 1700, 1800, 2600XM, 2800, 3700, 3800, and 7200 running Cisco IOS Release 12.4(11)T2; 7300, 7400, and 7600 running Cisco IOS Release 12.2(18)SXF8; 10000 and 12000 running 12.0(32)S7) running Cisco IOS and a Cisco Secure Access Control Server version 4.1.2.12, Cisco, submitted an Impact Analysis Report (IAR) to CCEVS for approval on 22 September 2009. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 1.0, February 2004. 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 10000 and 12000 routers running 12.0(32)S7 have reached end of life and the 7401 and 7600-MWAM have reached end of support. Therefore, these routers are not included in this maintenance effort.

From IOS 12.2(18)SXF8 to IOS 12.2(18)SXF16, 1485 minor fixes were applied and from IOS 12.4(11)T2 to IOS 12.4(15)T10, 6788 minor fixes were applied. Each fix was applied to make IPSec function as originally intended, no additional security functionality was added, and no existing security functionality was removed.

The vendor asserted each of the fixes fall into the following categorizations:

- Minor Changes with Little or No Security Relevance: These changes may be related to the TSC in some way, though may or may not relate directly to an SFR defined within the ST.

- Minor Changes with Some Security Relevance: These changes relate to the TSC in some way though the affect of the change is only to ensure the TOE functions as expected, and does not add or detract from the stated requirements in the ST. Therefore, changes in this category result in no adverse affect to the assurance baseline

The IAR provided by Cisco indicates the assurance evidence has been updated to reflect the changes, and appropriate testing of the changed TOE has occurred.

Conclusion:

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