**CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT**

# ASSURANCE CONTINUITY MAINTENANCE REPORT FOR CISCO ESR 5940 Running IOS Version 15.1(2)GC1 update to CISCO ESR 5940 Running IOS Version 15.2(3)GC

## Maintenance Update of Cisco ESR 5940 Running IOS Version 15.1(2)GC1 to CISCO ESR 5940 Running IOS Version 15.2(3)GC

**Maintenance Report Number:** CCEVS-VR-VID10429-2013

| | |
|---|---|
| **Date of Activity**: | 5 April 2013 |
| **References:** | Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;<br>Impact Analysis Report Common Criteria Assurance Maintenance Update of Cisco ESR 5940 Running IOS Version 15.1(2)GC1 to CISCO ESR 5940 running IOS Version 15.2(3)GC, VID:10429, Prepared by: Cisco Systems, Inc., version 0.3, March 2013. |

**Documentation Updated**: (List all documentation updated)

- Updated Security Target, Cisco 5940 Series Embedded Services Router Security Target, Revision 1.2, January 2013.
- Updated Configuration Management Documentation, Configuration Management, Lifecycle and Delivery Procedures for Cisco 5940 Series Embedded Services Router, Reference: ESR-CMP-v1-4, March 2013, Version: 1.5, EDCS-907672.
- Updated Guidance documentation, EDCS-984017, Cisco 5940 Series Embedded Services Router, Common Criteria Operational User Guidance and Preparative Procedures, Version 0.5, January 2013.

### Assurance Continuity Maintenance Report:

Cisco Systems, Inc. submitted an Impact Analysis Report (IAR) to CCEVS for approval on 10 January 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 is a purpose-built, routing platform that includes firewall, Intrusion Prevention, and VPN functionality. The firewall functionality included within the TOE provides the functionality specified in the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments. The TOE includes one router module that can operate in any CompactPCI (cPCI) 3 unit (3U) chassis. The Security Target, Configuration Management, Test, and Guidance documentation was updated to reflect bug fixes included in the new release of the product software. The only changes to the TOE were bug fixes that included both minor changes with little or no security relevance, i.e., changes that may be related to the TSC in some way, though may or may not relate directly to an SFR defined within the ST and minor changes with some security relevance, i.e., changes that relate to the TSC in some way though the effect 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. The changes resulted in no adverse effect to the assurance baseline.

The overall impact of the bug fixes was determined to be minor. Each fix was applied to make the TOE function as originally intended, no additional security functionality was added, and no existing security functionality was removed.

Examples of minor bug fixes that are not related to the TSC include:

- System load testing was not included in the scope of evaluation testing. Performance enhancements for greater system stability in high traffic situations or when thousands of ACL entries are applied were beyond the scope of intended usage.
- CLI improvements, corrections to options on commands, grammatical or syntax errors, and additions to help entries are irrelevant to the TSC.
- Modifications to optimize source code compilation
- Resource utilization fixes

Examples of minor bug fixes that are related to the TSC include:

- Fixes to firewall rule processing.
- Fixes to VPN flow control to ensure IOS functions as originally expected.

Test cases were rerun for the functional requirements in the following areas:

- Cryptography
- Firewall Information Flow
- Identification and Authentication
- Secure Management
- VPN Information Flow Control

No testing was run for Secure Auditing, Intrusion Prevention Services, GDOI, or VLAN Information Flow.

**Conclusion:**

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found it to be minor. In addition, the CCEVS requested that the vendor re-run the Intrusion Prevention Services tests and provide the test results for review. The test results indicated that there was no impact upon security. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.