ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS

Maintenance Update of Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS

Maintenance Report Number: CCEVS-VR-VID10692-2017

Date of Activity: 23 March 2017

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- Cisco IoT Industrial Ethernet and Connected Grid Switches Impact Analysis Report For Common Criteria Assurance Maintenance, Version 1.0, March 17, 2017
- collaborative Protection Profile for Network Devices, Version 1.0, 27-Feb-2015

Documentation reported as being updated:

- Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS Common Criteria Security Target, Version 2.0, 17 March 2017;
- Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS Common Criteria Operational User Guidance and Preparative Procedures, Version 2.0, 17 March 2107;
- Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS Hardware Entropy Information, Version 0.2, 17 March 2017.

Assurance Continuity Maintenance Report:

Cisco Systems, Inc., submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 16 March 2017. 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 IAR identifies the changes to the TOE included adding 2 new hardware components to the evaluated configuration and making related changes to various documents.

The evaluation evidence consists of the Security Target, Impact Analysis Report (IAR), User Guidance, and the entropy information document. The Security Target was revised to introduce the new pieces of supported hardware and the User Guide to identify those new hardware components. Likewise, the entropy document was updated to explain how the new hardware components contribute to the generation of cryptographic entropy. The IAR was new.

The evaluation was done against the collaborative Protection Profile for Network Devices and the ST referenced validated FIPS certificates. No changes were made in either the processor or the OS version and modifications were not required in any of the valid certificates.

Changes to TOE:

None, the IE4010 Series and IE5000 Series Hardware Models were added to the list of supported Hardware Models. No software updates were included.

Changes to Evaluation Documents:

- ST: Updated to add the IE4010 Series and IE5000 Series Hardware Models to the list of Hardware Models.
- AGD_PRE and OPE: Updated to add IE4010 Series and IE5000 Series Hardware Models.
- Entropy Information: Updated to add IE4010 Series and IE5000 Series Hardware Models.

  All these changes were made to address customer demands for the ability to procure new family hardware models and maintain the evaluated configuration.

Regression Testing:

The addition of the IE4010 Series and IE5000 to the list of supported hardware models did not require regression testing. However, the IE4010 and IE5000 models did undergo performance and functional testing to ensure the development specifications were met and that they operated correctly when installed and configured for use running the IOS 15.2(4)E software.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found them all to be minor. The inclusion of the IE4010 Series and IE5000 Series Hardware Models does not change any of the security functions that are claimed in the Security Target. All the security functions claimed are enforced by the Cisco IoT Industrial Ethernet and Connected Grid Switches software and not the hardware components.

The hardware modules are added to an existing series of supporting I/O modules. Those modules only served a functional role in the original evaluation so no security testing directly examined them. The vendor reported, however, that the new modules did undergo functional and performance testing.

In addition, the CCTL reported that there were no vulnerabilities associated with the IE4010 Series and IE5000 modules.

Therefore, CCEVS agrees that the original assurance is maintained for the product.