Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0937-2014-MA-01

Cisco Catalyst 6500-E Series Switches, Hardware models - WS-C6503-E, WS-C6504-E, WS-C6506-E, WS-C6509-E, and WS-C6513-E with Supervisor 2T (Sup2T) Cards (VS-S2T-10G or VS-S2T-10G-XL) Software version - IOS 15.1(1)SY1

from

Cisco Systems, Inc.

Common Criteria Recognition Arrangement

Common Criteria

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 and the developers Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-0937-2014.

The certified product itself did not change. The changes are related to an update of the Security Target.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0937-2014 dated 20 February 2014 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0937-2014.

Bonn, 14 April 2014

SOGIS IT SECURITY CERTIFIED

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 99 9582-0 - Fax +49 228 9582-5477 - Infoline +49 228 99 9582-111

Assessment

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements* [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [3], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the Cisco Catalyst 6500-E Series Switches, Hardware models - WS-C6503-E, WS-C6504-E, WS-C6506-E, WS-C6509-E, and WS-C6513-E with Supervisor 2T (Sup2T) Cards (VS-S2T-10G or VS-S2T-10G-XL) Software version - IOS 15.1(1)SY1, Cisco Systems, Inc., submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. In accordance with those requirements, the IAR describes (i) the changes made to the certified TOE, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The certified product itself did not change. The changes are related to an update of the Security Target. The updated Security Target claims strict, instead of demonstrable, conformance to the following Common Criteria Protection Profile: US Government, Security Requirements for Network Devices, version 1.0, dated 10 December 2010.

Conclusion

The change has no effect on assurance. The Security Target [5] was updated.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

Therefore, BSI agrees that the assurance as outlined in the Certification Report [3] is maintained for this version of the product.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0937-2014 dated 20 February 2014 is of relevance and has to be considered when using the product.

Additional obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

This report is an addendum to the Certification Report [3].

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Cisco Catalyst 6500-E Series Switch Impact Analysis Report For Common Criteria Assurance Maintenance, Version .01, EDCS-1399878, 2014-4-10, Cisco Systems, Inc., CISCO CONFIDENTIAL

[3] Certification Report BSI-DSZ-CC-0937-2014 for “Cisco Catalyst 6500-E Series Switches - Cisco IOS Software, Version 15.1(1)SY1, RELEASE SOFTWARE (fc5) from Cisco Systems, Inc.”, Bundesamt für Sicherheit in der Informationstechnik, Version 1.1, 20 February 2014

[4] Security Target BSI-DSZ-CC-0937-2014, Version: 1.0, 2014-02-14, ST for Cisco Catalyst 6500-E Series Switches, EDCS 1252106, Cisco Systems, Inc.

[5] Security Target BSI-DSZ-CC-0937-2014, Version: 1.1, 2014-02-28, ST for Cisco Catalyst 6500-E Series Switches, EDCS 1252106, Cisco Systems, Inc.