CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Cloud Services Router 1000V (CSR1000V), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K) running IOS-XE Version 17.3

Maintenance Report Number: CCEVS-VR-VID11186-2022

Date of Activity: July 29, 2022

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." 29 August 2014.

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K) running IOS-XE Version 17.6 Security Target, Version 2.0, June 6, 2022

Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K) running IOS-XE Version 17.6 CC Configuration Guide, Version 2.0, June 6, 2022

Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Cloud Services Router 1000V (CSR1000V), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K) running IOS-XE Version 17.3 Impact Analysis Report Update IOS-XE 17.3 to 17.6, Version 0.3, July 29, 2022

Description of Changes:

The changes made to the evaluated TOE since the Common Criteria evaluation in December 2021 (CCEVS-VR-VID11186-2021) are described here.

- Removal of hardware model Cisco Cloud Services Router 1000V (CSR1000V) from the evaluated configuration
- Update of TOE software version from IOS-XE 17.3 to IOS-XE 17.6
- Updates to the Security Target (ST):
    - Updated to reflect IOS-XE version 17.6 software version number.
    - Updated to remove any references to CSR1000V and vND.
    - Updated sections 5.3.2.10 and 6.1 to remove the 'software-based noise source' selection from FCS_RBG_EXT.1.2 because the removed CSR1000V is the only model that claimed a software-based noise source.
- Updates to the Administrative Guidance Document (AGD):
    - Updated to reflect IOS-XE version 17.6 software version number.
    - Updated the image names and hashes in the list of evaluated software images

Changes to TOE:

Hardware Changes**:**

No changes to hardware other than removal of the CSR1000V from the evaluated configuration.

- Evaluated TOE Hardware Models: Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Cloud Services Router 1000V (CSR1000V), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K)
- Changed TOE Hardware Models: Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K)

Software Changes**:**

- Evaluated TOE Software Version: IOS-XE 17.3
- Changed TOE Software Version: IOS-XE 17.6

The TOE version updates include 37 new features and 219 bug fixes have been found to either not have any security relevance or do not fall within the scope of the evaluated functionality. Of these 219 bug fixes:

- Related to features/components outside the CC evaluated configuration: 114
- Related to implementation of functionality that is not claimed in the TSF: 33
- Related to ensuring that the TOE functions as expected, but below the level of visibility to assurance activities: 72

Information on the specific updates can be found in detail in Appendix B and Appendix C of the IAR. The following is a summary of the new features introduced with the TOE software update:

- Optional features not part of the evaluated configuration, and disabled by default
    - Network-Based Application Recognition (NBAR) support
    - Distributed Anycast Gateways (DAG)

    - Performance Management (PM)
    - Micro-BFD support
    - Dynamic ARP Inspection (DAI)
    - IPv6 First Hop Security
    - Dynamic Core Allocation
- Features that add support for functionality that do not impact TOE security functions
    - Performance related enhancements including added support for L2VPN, L3VPN and service-group together on port-channel interfaces in QOS Policies
    - Support for global address within static NAT and static PAT
    - Enhancements to the BGP routing protocol
    - Added support for Stateless Static NAT
    - Enhancements to the IS-IS routing protocol
    - Enhancements to the punt policing and monitoring feature
    - Enhancements to IPv6 Mroutes
    - Enhancements to EVPN VXLAN
    - Added support for Segment Routing Flexible Algorithm with IS-IS
    - Enhancements to interface speed
    - Enhancements to SR-TE Policy
    - Added support for Tunnel Path MTU discovery on MPLS-enabled GRE tunnel
    - Enhancements to show commands
    - Added support for Asymmetric Lease for DHCPv6 Relay Prefix Delegation
    - Added support for System Reports
    - Enhancements to breakout cable support
- Features that pertain to functionality not included in the Common Criteria evaluation
    - Configuring Smart Licensing using Web UI – Web UI is not included
    - Configuring Encapsulated Remote Switching Port Analyzer (ERSPAN) – Cisco DNA is not included
    - Secure Factory Reset – not included
    - IEEE802.1ad Support on Port-channel and Subinterfaces – IEEE802.1ad is not included
    - Layer 2 Protocol Tunneling on Ports – Layer 2 Protocol Tunneling is not included
    - Consent Token Authorization Process for Dev Key Access – Consent Token Authorization Process is not included
    - L2VPN Traffic SteeringUsing SR-TE Preferred Path – VPWS or VPLS are not included
    - Zone-Based Firewall Reclassification – Zone-Based Firewall (ZBFW) is not included

Changes to the IT Environment:

None

Changes to the Development Environment:

None

Affected Evidence:

- Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Cloud Services Router 1000V (CSR1000V), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K) running IOS-XE Version 17.3 Security Target, Version 1.0, December 28, 2021
- Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K) running IOS-XE Version 17.3 CC Configuration Guide, Version 0.5, December 28, 2021

Description of ALC Changes:

Changes to the following documents were made:

- ST
    - From: Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Cloud Services Router 1000V (CSR1000V), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K) running IOS-XE Version 17.3 Security Target, Version 1.0, December 28, 2021
    - To: Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K) running IOS-XE Version 17.6 Security Target, Version 2.0, June 6, 2022
- AGD
    - From: Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K) running IOS-XE Version 17.3 CC Configuration Guide, Version 0.5, December 28, 2021
    - To: Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 1100 Series (ISR1100), Cisco Integrated Services Router 4200 Series (ISR4K) running IOS-XE Version 17.6 CC Configuration Guide, Version 2.0, June 6, 2022

Assurance Continuity Maintenance Report:

- Cisco Systems, Inc. submitted an Impact Analysis Report to remove the CSR1000V hardware model from the evaluated configuration, as well as update the TOE software to IOS-XE 17.6.
- The IAR specifies that there are 37 new features and 219 bug fixes in the changed TOE. These updates are all either not security-relevant or are not within the scope of the original evaluated functionality.
- There are no changes to the development environment.
- The ST and AGD were updated as a result of updating the TOE software version and removal of the CSR1000V hardware model.
- The processors specified as the platform in the ST is reported at the microarchitecture level and is an identical match to the processors specified on the CAVP certificate, certificate number A1462. The implementation of the validated cryptographic algorithm has not been modified upon integration into the TOE, as the Cisco IC2M Rel5a is used in both the IOS-XE

17.3 and 17.6 versions. Therefore, the cryptographic algorithm implementation validated for CAVP conformance also applies to the changed TOE.

Description of Regression Testing:

During development of a new IOS-XE version, there are various tests performed to ensure the product performs as expected. Bug fixes and new features are tested to ensure the feature works as expected or the fix was effective. Additionally, regression testing, using pre-defined test cases, is performed to ensure that overall product performs as expected, ensuring existing features and functionality from previous versions was not broken in the development of the latest version.

Based on the bug testing and regression testing, Cisco believes the product behaves as expected, and that the newer version conforms to the claims set forth in the initial Common Criteria Evaluation.

Vulnerability Assessment:

A search of the following national sites was conducted:

https://nvd.nist.gov/vuln/search
https://www.cisco.com/
https://tools.cisco.com/security/center/softwarechecker.x

The following key words, product, and vendor were each selected as search criteria for vulnerabilities related to the TOE:

- Cisco Router
- Cisco IOS XE 17.3
- Aggregation Services Router
- ASR 1K
- ASR1002-X
- Intel Xeon EC3539
- ASR1006
- Intel Xeon L5238
- Integrated Services Router
- ISR 1100
- C1111
- ARMv8
- ISR 4K
- ISR4221
- Intel Atom C2558
- IOS XE IPSec
- IOS XE SSH
- IOS VPN
- Cisco IC2M
- IOS Common Cryptographic Module

- TCP
- UDP

Vendor:

- Cisco

The IAR contains the output from the vulnerability searches and the rationale why the search results are not applicable to the TOE. This search was performed on July 12, 2022. No vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

Section 2.1.1 of the IAR describes how a TOE hardware model was removed from the TOE evaluated configuration.

Section 8 of the IAR summarizes the changes made for this assurance maintenance activity. This section describes that all new features and bug fixes are considered to have minor impact due to having no security relevance or no direct relation to the SFRs defined in the ST.

Based on this and other information from within the IAR document, the vendor has concluded that the overall impact is **minor**.

Validation Team Conclusion:

The validation team reviewed the changes and concurred the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The updated ST changed to remove a hardware model and the ST and AGD were updated to reflect the TOE software update. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.