ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Cisco Aggregation Services Router 1004 (ASR1K)

Maintenance Update of Cisco Aggregation Services Router 1004 (ASR1K)

Maintenance Report Number: CCEVS-VR-VID10950-2019

Date of Activity: 27 August 2019

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, 12 September 2016 Version 3.0;
- Impact Analysis Report for Cisco Aggregation Services Router 1004 (ASR1K). Impact Analysis Report for Common Criteria Assurance Maintenance, Version 0.1, August 16, 2019
- collaborative Protection Profile for Network Devices (NDcPP) + Errata 20180314, Version 2.0e

Documentation reported as being updated:

- Cisco Aggregation Services Router 1004 (ASR1K) Security Target, Version 2, 16 August 2019.
- Cisco Aggregation Services Router 1000 Series (ASR1k) Common Criteria Configuration Guide, Version 2.0, 16 August 2019.

Assurance Continuity Maintenance Report:

Cisco Systems, Inc., submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 16 August 2019. 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 3.0. 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 software changes (bug fixes and feature updates) and making related changes to various documents.

The evaluation evidence consists of the Security Target, Impact Analysis Report (IAR), and Configuration Guidance. The Security Target was revised to reflect the new IOS-XE version 16.12 software version number. The Configuration Guide was revised to reflect the new IOS-XE version 16.12.1a software version number. There were no other changes made to the ST or Configuration Guide.

Changes to TOE:

The IOS-XE software was updated from 16.9 to 16.12.1a. These updates were bug fixes and feature updates.

Changes to Evaluation Documents:

- ST: Modified IOS-XE version number from 16.9 to 16.12.
- Configuration Guide: Modified IOS-XE version number from 16.9 to 16.12.1a.

Regression Testing:

Each individual change was unit tested, and the IOS-XE 16.12.1a software image has had a limited amount of automated regression testing covering all major areas of baseline client functionality.

Vulnerability Analysis:

A new vulnerability analysis was run and as of 8/16/2019 all vulnerabilities have been addressed by the new IOS-XE 16.12.1a version.

Vulnerability	Cisco distributed defect tracking system (DDTS) Identifier	Release version that addresses the Vulnerability
CVE-2019-1862 - A vulnerability in the web-based user interface (Web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker to execute commands on the underlying Linux shell of an affected device with root privileges.	CSCvn20358	HTTP Server feature is not a TSF claim included in the TOE. Cisco addressed this vulnerability in IOS-XE 16.12.1a.
CVE-2019-1762 - A vulnerability in the Secure Storage feature of Cisco IOS and IOS XE Software could allow an authenticated, local attacker to access sensitive system information on an affected device.	CSCvi66418	Cisco addressed this vulnerability in IOS-XE 16.12.1a.
CVE-2019-1761 - A vulnerability in the Hot Standby Router Protocol (HSRP) subsystem of Cisco IOS and IOS XE Software could allow an unauthenticated, adjacent attacker to receive potentially sensitive information from an affected device.	CSCvj98575	Cisco addressed this vulnerability in IOS-XE 16.12.1a
CVE-2019-1759 - A vulnerability in access control list (ACL) functionality of the Gigabit	CSCvk47405 CSCvm97704	Cisco addressed this vulnerability in IOS-XE 16.12.1a.

Ethernet Management interface of Cisco IOS XE Software could allow an unauthenticated, remote attacker to reach the configured IP addresses on the Gigabit Ethernet Management interface.		
CVE-2019-1755 - A vulnerability in the Web Services Management Agent (WSMA) function of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary Cisco IOS commands as a privilege level 15 user.	CSCvi36824	Cisco addressed this vulnerability in IOS-XE 16.12.1a.
CVE-2019-1754 - A vulnerability in the authorization subsystem of Cisco IOS XE Software could allow an authenticated but unprivileged (level 1), remote attacker to run privileged Cisco IOS commands by using the web UI.	CSCvi36813	The web UI is not a TSF claim included in the TOE. Cisco addressed this vulnerability in IOS-XE 16.12.1a.
CVE-2019-1752 - A vulnerability in the ISDN functions of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause the device to reload.	CSCvk01977	Cisco addressed this vulnerability in IOS-XE 16.12.1a.
CVE-2019-1745 - A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with elevated privileges.	CSCvj61307	Cisco addressed this vulnerability in IOS-XE 16.12.1a.
CVE-2019-1743 - A vulnerability in the web UI framework of Cisco IOS XE Software could allow an authenticated, remote attacker to make unauthorized changes to the filesystem of the affected device.	CSCvi48984	The web UI is not a TSF claim included in the TOE. Cisco addressed this vulnerability in IOS-XE 16.12.1a.
CVE-2018-15372 - A vulnerability in the MACsec Key Agreement (MKA) using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) functionality of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to bypass authentication and pass traffic through a Layer 3 interface of an affected device.	CSCvh09411	MACsec is not a TSF claim included in the TOE. Cisco addressed this vulnerability in IOS-XE 16.12.1a.
CVE-2017-6665 - A vulnerability in the Autonomic Networking feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to reset the Autonomic Control Plane (ACP) of an affected system and view ACP packets that are transferred in clear text within an affected system, an Information Disclosure Vulnerability.	CSCvd51214	The Autonomic Networking feature is not a TSF claim included in the TOE.
CVE-2017-6663 - A vulnerability in the Autonomic Networking feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause autonomic nodes of an affected system to reload, resulting in a denial of service (DoS) condition.	CSCvd88936	The Autonomic Networking feature is not a TSF claim included in the TOE.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor.

In addition, the CCTL reported that there were no vulnerabilities associated with the new software version, IOS-XE 16.12a.

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