ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Ciena, Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2

Maintenance Update of Ciena, Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2

Maintenance Report Number: CCEVS-VR-VID10460-2014

Date of Activity: 30 May 2014

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;

Impact Analysis Report for Ciena, Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2, version 1.0, 12 March 2012.

Documentation Updated:

The following assurance evidence was affected by the release of Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 and resulted in updated documentation:

Security Target – Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.9 and 7.1 Security Target v1.6.

Release Notes – The release notes below were created for each patch between Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.9 and 7.1 to 6.10.2 and 7.2. They contain a listing of the new features implemented and bug fixes addressed between the validated TOE and the changed TOE.

- SAOS Release Notes Release 6.9.1.148 (009-3202-013_(SAOS_R6.9.1_Customer_release_Notes)RevF.pdf)
- 39XX/51XX Service Delivery and Aggregation Switches Release Notes Release 6.10.0.294 (009-3203-013_(39XX_51XX_R6.10.0_Customer_Release_Notes)RevC.pdf)
- 39XX/51XX Service Delivery and Aggregation Switches Release Notes Release 6.10.1.148 (009-3203-013_(39XX_51XX_R6.10.1_Customer_Release_Notes)RevG.pdf)
- 39XX/51XX Service Delivery and Aggregation Switches Release Notes Release 6.10.2.140 (009-3203-013_(39XX_51XX_SAOS_R6.10.2_Customer_Release_Notes)RevN.pdf)
- 5410 Service Aggregation Switch Release Notes Release 7.1.1.278 (009-3201-013_(5410_R7.1.1 _Release_Notes)RevB.pdf)
- 5410 Service Aggregation Switch Release Notes Release 7.2.0.531 (009-3218-013_(5410_R7.2 _Release_Notes)RevB.pdf)

End-user Guidance Documents:

- Evaluated Configuration for Ciena ActivEdge Service Delivery/Aggregation Switch with SAOS versions 6.10.2 and 7.2, March 2014
- 39XX/51XX Service Delivery and Aggregation Switches Configuration Release 6.10, Revision E, April 2013
- 39XX/51XX Service Delivery and Aggregation Switches Administration and Security Release 6.10, Revision E, April 2013
- 5410 Service Aggregation Switch Administration and Security Release 7.2, Revision B, December 2012
- 5410 Service Aggregation Switch Configuration Release 7.2, Revision A, October 2012
- 5410 Service Aggregation Switch Command Reference Release 7.2, Revision A, October 2012
- 5410 Service Aggregation Switch Fault and Performance Release 7.2, Revision B, December 2012
- 5410 Service Aggregation Switch Software Management and Licensing Release 7.2, Revision A, October 2012

Assurance Continuity Maintenance Report:

Booz Allen Hamilton CCTL, on behalf of the Ciena Corporation, submitted an Impact Analysis Report (IAR) to CCEVS for approval on 12 March 2014. 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 includes a series of switches and related components, i.e., the Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 (hereafter referred to as CES). The TOE receives data from an external source and forwards that data to one or many ports. CES is part of the Carrier Ethernet technology. Carrier Ethernet provides a way to deliver Ethernet services across many networks while providing bandwidth management. CES operates on Quality of Service (QoS) capabilities and virtual switching functions to deliver different amounts of data to various ports. CES also supports next-generation Ethernet features that transport different Ethernet services through fiber or copper connections.

Security Target and guidance documentation was updated to reflect the changes that were incorporated in more recent releases of the TOE's software. The evaluated releases of the TOE will be updated from 6.9 to 6.10.2 and from 7.1 to 7.2. Regression testing was performed using the vendor's functional/security test procedures that were approved by the original evaluation and the actual results were recorded as part of the test documentation.

The Release Notes listed above included new features and bug fixes. The new features were found to have a minor or no security impact. There are no changes that change the implementation of SFRs, remove the enforcement of existing SFRs, or force the addition of any security-relevant functionality or interfaces. The vast majority of changes are enhancements to the TOE's switching capability. These enhancements would not fundamentally change the ability of the TOE to isolate different streams of network traffic and determine where to send them to based on certain attributes of the traffic data.

The product changes that were reviewed are those that were within the scope of the original validated TOE. Capabilities outside of the original TOE boundary were considered to be non-applicable. In particular, the following potential security-related product changes were not reviewed as part of this effort:

6.x

- IPv6 support for management plane traffic
- Enhanced MPLS services
- Larger variety of supported optical transceivers
- VLAN enhancements (ability to add VLAN tag to mirrored ports, TWAMP, UNI EVPL services, PFG support)

7.x

- Rolling upgrade capability to minimize downtime during software updates
- Larger variety of supported optical transceivers
- Enhanced MPLS services

Some of the new features were relevant to the scope of the original TSF. The ST was updated to reflect minor changes to the functionality introduced by these new features. Those ST changes are listed below.

While there were numerous bug fixes, none of these bugs were identified in security-relevant behavior during initial validation testing. Some fixes apply to very specific boundary case scenarios that are not likely to occur. Others apply to issues that were at a lower level of detail than what was tested for EAL2. In general, the security-relevant bug fixes do not change how the TSF is implemented so much as they allow the TOE to implement the TSF in a manner that is consistent with what the Security Target defines. Many bug fixes were not considered to be security relevant because they represent changes to functionality that was not included as part of the TSF or were considered to be general performance/diagnostic/stability issues that were unrelated to security.

Changes to Security Target related to Release 6.10.2:

Password Enhancements: Increased string length for username and password as follows: • RADIUS authentication - 32 characters for username and 128 characters for password • TACACS authentication - 32 characters for username and 128 characters for password • SSH, Telnet and console sessions - 32 characters for username and 128 characters for password when using RADIUS and TACACS authentication and 16 characters for username and 16 characters for password for local authentication Impacts: The guidance was updated to reflect the updated version number for the TOE. The Administration and Security Guide was updated to lists the username and password length constraints. The ST did not specify username or password constraints and was not updated.
RADIUS authentication grants login privileges based on Vendor Specific Attributes (VSAs) Impact s: RADIUS is already defined as granting authentication privileges in the ST but additional clarification as to how those privileges are derived has been included. A discussion of the new feature was included in the configuration guidance but is not applicable to the administration and security guidance, which is the primary focus for security-relevant guidance.
Security Management: Support for the "admin" user access level. Impact s: The ST and administrative guidance were updated to discuss the “admin” user access level for both versions of the TOE. The method of enforcement of the SFR remains the same and is now in fact consistent between the two versions of the TOE.
Bug SSH_SFTP – JE-28912: The SFTP server process is disabled by default. The system supports the ability to enable, disable, and display SFTP settings with the following commands: system server sftp disable system server sftp enable system server sftp show Impacts: The change puts the TOE in a more secure configuration by default. The supplemental guidance was updated.

Changes to Security Target related to Release 7.2:

System now allows for user names of up to 32 characters and password length of up to 128 characters.

- System provides command interface to suppress RADIUS/TACACS login authentication message: `Waiting for authentication server reply.
- System SFTP server is now disabled by default, thereby closing a security hole for access to the kernel.

Impact s: The guidance was updated to reflect the updated version number for the TOE. The Administration and Security Guide lists the username and password length constraints. Additionally, the guidance to manually disable the SFTP server is no longer applicable so it has been removed from the supplemental guidance. The ST did not specify username or password constraints and was not updated.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found it to be minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.