CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches Running Junos 12.1.R3.6

Maintenance Report Number: CCEVS-VR-VID10517-2014a

Date of Activity: 29 May, 2014

References: Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 2, September 8, 2008

Common Criteria document CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements” Version 1, February 2004

Security Requirements for Network Devices, Version 1.1, 08 June 2012 [NDPP]

Impact Analysis Report Junos 12.1R3.6, Version 1.0, May 12, 2014

Affected Evidence: Security Target: Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running Junos12.1R3.5, Version 1.6, January 7, 2014

Security Target Annex A, Version 1.5

Junos OS Secure Configuration Guide for Common Criteria Network Device Protection Profile for Devices Running Junos OS 12.1.

Updated Developer Evidence:

Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running Junos 12.1R3.6

Security Target Annex A, Version 1.6

Junos OS Common Criteria Evaluated Configuration Guide for EX Series, M Series, MX Series, and T Series Devices Release 12.1R3.6, 2014-05-13

Assurance Continuity Maintenance Report:

This 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, September 8, 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence that was updated as a result of those changes, and the security impact of those changes.

Changes to TOE:

There has been a single change to the Junos 12.1R3.6 TOE since the validation of the Junos 12.1R3.5 TOE:

A vulnerability fix to address the vulnerability that a crafted TCP packet passed to the Routing Engine could lead to a kernel crash. Specifically, the Junos kernel may crash when a specifically crafted TCP packet is received by the Routing Engine (RE) on a listening TCP port. TCP traffic traversing the router will not trigger this crash. Only TCP packets destined to the router itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the crash. This issue can be triggered by both IPv4 and IPv6 TCP packets destined to the RE. This vulnerability is documented in the Juniper Security Incident Response Team’s (SIRT) technical bulletin at: http//kb.juniper.net/InfoCenter/index?page=content&id=JSA10550.

To address the issue, a few discrete new lines of code were introduced in a single source code file to address this TCP option processing issue.

Vendor Conclusion: This change is considered to be minor in the context of the SFRs claimed in the security target for Junos12.1R3.5 TOE. The change does not directly impact the enforcement of any of the SFRs, and serves to correct an operational vulnerability in the product so that it is more stringent in meeting the implemented RFCs. The developer successfully completed regression testing of the Junos 12.1R3.6 release in accordance with their quality management and rigorous product lifecycle NPI.

Validation Team Conclusion: The change to the TOE is confined to a single code change to a single software file. The vendor claims that testing of the specific changes and a set of regression testing was conducted. Those test logs and supporting evidence were not provided in the IAR package. The validation team concurs the change was functional in nature.

The validators reviewed the changes and concur that the changes should be should be classified as minor and that certificate maintenance is the correct path for assurance continuity. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.