Maintenance Report

SonicOS Enhanced v6.2.0 on NSA Series and SM Series Appliances

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-7-121 MR
Version: 1.0
Date: 28 April 2015
Pagination: 1 to 2

1 Introduction

Dell Software, Inc. has submitted the Impact Analysis Report (IAR) for SonicOS Enhanced 6.2.0 on NSA Series and SM Series Appliances (hereafter referred to as Sonic OS), satisfying the requirements outlined in Assurance Continuity: CCRA Requirements, v2.1, June 2012. In accordance with those requirements, the IAR describes the changes implemented in Sonic OS, (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

2 Description of changes in the Maintained Target of Evaluation

The following characterizes the changes implemented in Sonic OS. For each change, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted by the developer to ensure that the assurance in the Target of Evaluation (TOE) was maintained. The changes in Sonic OS comprise;

- Support for IPv6;
- Support for Jumbo Frame;
- Support for Portshield Groups;
- Support for layer 2 switching;
- Support for 3G/4G wireless WAN (Wide Area Network);
- Advanced bandwidth management;
- Client content filtering service;
- bug fixes and feature enhancements resulting from defects detected and resolved through the QA/test process; and
- The appliances now covered by the changed TOE are the following SonicWALL appliances:
    - SM 9600;
    - SM 9400;
    - SM 9200;
    - NSA 6600;
    - NSA 2600;
    - NSA 3600;
    - NSA 4600; and
    - NSA 5600.

3 Description of Changes to the IT Environment

The following changes were made to the underlying IT environment;

The following Web browsers are now supported:

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display);
- Firefox 16.0 and higher;
- Internet Explorer 8.0 and higher (do not use compatibility mode); and
- Safari 5.0 and higher.

4 Affected developer evidence

Modifications to the product necessitated changes to a subset of the developer evidence that was previously submitted for the TOE. The set of affected developer evidence was identified in the IAR.

Modifications to the security target were made to reflect the new product versions.

5 Conclusions

Through functional and regression testing of Sonic OS, assurance gained in the original TOE certification was maintained. As all of the changes to the maintained TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance continuity and re-evaluation is not required.

6 References

- Assurance Continuity: CCRA Requirements, v2.1, June 2012;
- CCS Guide #6, Technical Oversight for Assurance Continuity of a Certified TOE, v1.6, May 2011;
- Certification report for SonicWALL SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances, version 1.1, 2 July 2014;
- Dell SonicWALL, Inc. SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances Security Target, version 2.5, 27 June 2013