CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances Security

Maintenance Report Number: CCEVS-VR-VID11028-2020

Date of Activity: 17 August 2020

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." March 20, 2013

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

SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances Impact Analysis Report for Common Criteria Assurance Maintenance Version 1.0 June 2020

SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances Security Target Version 1.10, June 2020 (FWcPP)

SonicWall® SonicOS 6.5 Common Criteria Addendum Version 1.5 June 2020

Affected Evidence:

SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances Security Target Version 1.10, June 2020 (FWcPP)

Updated Developer Evidence:

There is no change to the developer evidence of the validated TOE. There were no software code changes.

Description of ASE Changes:

SonicWall, Inc., submitted an Impact Analysis Report (IAR) to CCEVS for approval to add one new hardware model: TZ350. This model is identical to the already included TZ350W with the exception that the TZ350 does not include any wireless interfaces. All other hardware specifications including the processor are identical.

Changes to TOE:

There are no changes to the TOE. The only change is to add an additional hardware model, TZ350; identical to the TZ350W without the wireless interface.

The TZ350 hardware is effectively a subset of the already included TZ350W. The hardware does not introduce any new interfaces into the evaluation. The software that runs on the TZ350 is identical to the software that runs on the other hardware model within the evaluation.

The hardware includes the same processor as other already included hardware models (Cavium Octeon III CN7020-800). Because the hardware uses identical components as the already included TZ350W, no new device drivers are introduced into the product.

Description of ALC Changes:

The only change to the security target were the addition of hardware model TZ350 and the update of the version number.

- SonicWall SonicOS V6.5.4 with VPN and IPS on TZ and SOHO, Security Target Version 1.10, June 2020 (FWcPP)

The guidance document was also updated with the addition of hardware model TZ350 and the update of the version number.

- SonicWall® SonicOS 6.5 Common Criteria Addendum, Version 1.5, June 2020

Assurance Continuity Maintenance Report:

- SonicWall, Inc. submitted an Impact Analysis Report (IAR) for the addition of one hardware model, TZ350, described above.
- There were no code changes and, therefore, there was no impact on the developer evidence of the validated TOE.
- There are no changes to the development environment.
- The changes to the ST and other documents were limited to document version with the addition of the new hardware model.

Description of Regression Testing:

In addition to the vendor performing vulnerability testing, functional regression testing and unit testing is also performed against each release and/or software build to ensure the TOE functionality is maintained and that the source code is fit for use.

The regression testing performed against the TOE includes partial automation testing as well as manual test execution by the Quality Assurance Team within SonicWall. This testing ensures that the functionality claimed within the Security Target has not been impacted.

The unit testing is performed against each software build to ensure that the source code used in each release is fit for use and performing in the expected manner.

For instances when security related bugs were identified, the vendor performed specific testing on the updates to ensure that the identified behavior is no longer present within the TOE and the TOE operates as expected. For example, when bugs related to memory leaks are incorporated into the TOE software, the vendor performs the operations that resulted in the memory leak to ensure that the operations no longer result in the memory leak. After this is successfully confirmed, the testing is incorporated into the regular regression testing and rerun until the TOE software is released.

Vulnerability Assessment:

The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

- http://nvd.nist.gov/
- https://www.cvedetails.com/
- http://www.kb.cert.org
- www.securiteam.com
- http://nessus.org
- http://www.zerodayinitiative.com
- https://www.exploit-db.com/
- https://www.rapid7.com/
- Vendor website

The evaluator selected the 27 search key words based upon the vendor name, the product name, and key platform features the product leverages. The search terms used were:

- SonicWall SonicOS Enhanced v6.5.4
- SonicWall
- TZ 300P
- TZ 350W
- TZ 350
- TZ 600P
- SOHO 250
- SOHO 250W
- SOHO
- TZ
- TLS 1.1
- TLS 1.2
- IPSEC
- HTTPS
- Firewall
- TCP
- UDP
- IPv4
- IPv6
- ICMPv4
- ICMPv6
- VPNGW
- VPN
- IPS
- Cavium Octeon III CN7020-800

- Cavium Octeon III CN7130-1400
- Cavium Octeon

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 6/23/2020. No vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

The TZ350 hardware is effectively a subset of the already included TZ350W. The hardware does not introduce any new interfaces into the evaluation. The software that runs on the TZ350 is identical to the software that runs on the other hardware model within the evaluation.

The hardware includes the same processor as other already included hardware models (Cavium Octeon III CN7020-800). Because the hardware uses identical components as the already included TZ350W, no new device drivers are introduced into the product.

Based on all this, the newly added hardware is equivalent to the previously included hardware and this is a non-security relevant change.

Validation Team Conclusion:

The validation team reviewed the changes and concur the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The updated Security Target was only changed to add the hardware model, TZ350. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.