CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

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

Maintenance Report Number: CCEVS-VR-VID11028-2021 (FWcPP)

Date of Activity: 29 September 2021

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, NSa, and SM Appliances Impact Analysis Report for Common Criteria Assurance Maintenance Version 1.0 August 2021

SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ , SOHO, NSa, and SM Appliances Security Target Version 2.0, August 2021 (FWcPP)

SonicWall® SonicOS 6.5 Common Criteria Addendum Version 2.0 August 2021

Affected Evidence:

SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ , SOHO, NSa, and SM Appliances Security Target Version 2.0, August 2021 (FWcPP)

SonicWall® SonicOS 6.5 Common Criteria Addendum Version 2.0 August 2021

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 23 new hardware models, as shown in the 'hardware differences' table below, with 14 new Cavium Octeon II/III processors all using the same MIPS64 microarchitecture as processors included in the original evaluation (also shown in the table below). The ST identifies CAVP C743, which was specified on the original evaluation and the assurance maintenance of August 2020. The processor families do appear in the CAVP. There are no software changes.

Differences in Hardware		
Model	**Processor**	**Analysis**
TZ 300	Cavium Octeon III CN7020-800	This processor uses the same MIPS64 microarchitecture as processors included in the original evaluation. This processor was also used in the previous evaluation.
TZ300W	Cavium Octeon III CN7020-800	This processor uses the same MIPS64 microarchitecture as processors included in the original evaluation. This processor was also used in the previous evaluation.
TZ400	Cavium Octeon III CN7130-800	This processor uses the same MIPS64 microarchitecture as processors included in the original evaluation. The differences between this processor and previously included processors include number of cores and speed.
TZ400W	Cavium Octeon III CN7130-800	This processor uses the same MIPS64 microarchitecture as processors included in the original evaluation. The differences between this processor and previously included processors include number of cores and speed.
TZ500	Cavium Octeon III CN7130-1000	This processor uses the same MIPS64 microarchitecture as processors included in the original evaluation. The differences between this processor and previously included processors include number of cores and speed.
TZ500W	Cavium Octeon III CN7130-1000	This processor uses the same MIPS64 microarchitecture as processors included in the original evaluation. The differences between this processor and previously included processors include number of cores and speed.
TZ600	Cavium Octeon III CN7130-1400	This processor uses the same MIPS64 microarchitecture as processors included in the original evaluation. This processor was also used in the previous evaluation.
NSa 2650	Cavium Octeon III CN7130-1600	This processor uses the same MIPS64 microarchitecture as processors included in the original evaluation. The differences between this processor and previously included processors include number of cores and speed.
NSA 3600	Cavium Octeon II CN6635-800	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
NSa 3650	Cavium Octeon III CN7130-1600	This processor uses the same MIPS64 microarchitecture as processors included in the original evaluation. The differences between this processor and previously included processors include number of cores and speed.
NSA 4600	Cavium Octeon II CN6640-1100	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.

NSa 4650	Cavium Octeon II CN6645-1200	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
NSA 5600	Cavium Octeon II CN6645-1300	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
NSa 5650	Cavium Octeon II CN6645-1500	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
NSA 6600	Cavium Octeon II CN6870-1000	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
NSa 6650	Cavium Octeon II CN6870-1200	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
NSa 9250	Cavium Octeon II CN6870-1200	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
NSa 9450	Cavium Octeon II CN6880-1400	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
NSa 9650	Cavium Octeon II CN6880-1400	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
SM 9200	Cavium Octeon II CN6870-1000	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
SM 9400	Cavium Octeon II CN6880-1200	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
SM 9600	Cavium Octeon II CN6880-1200	The differences between this processor and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
SM 9800	Cavium Octeon II CN6640-1100 Cavium Octeon II CN6880-1200	The differences between these processors and previously included processors include number of cores, speed, fewer I/O options (not leveraged by the product family), and less built-in storage. These are lower performance options.
Summary	The differences between the hardware included in the original evaluation and the additional hardware is only performance related and do not affect the implemented evaluated security functionality.	

Changes to TOE:

There are no changes to the TOE. The only change is to add 23 additional hardware models with 14 new processors.

Description of ALC Changes:

The only change to the security target were the addition of 23 hardware models as shown in the table above and the update of the version number.

- SonicWall SonicOS V6.5.4 with VPN and IPS on TZ and SOHO, Security Target Version 2.0, August 2021 (FWcPP-epIPS-epVPNGW)

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

- SonicWall® SonicOS 6.5 Common Criteria Addendum, Version 2.0, August 2021

Assurance Continuity Maintenance Report:

- SonicWall, Inc. submitted an Impact Analysis Report (IAR) for the addition of 23 hardware models, 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:

The vendor performs full functional and regression testing against all new hardware released. Full testing, including testing of the evaluated security functionality was tested by the SonicWall, Inc.

Functional regression and unit testing is also performed against each release and hardware build to ensure the TOE functionality is maintained and that the product is fit for use. This functional testing included verification that any newly introduced feature does not affect the security functionality previously tested and verified. This testing ensures that the functionality claimed within the Security Target has not been impacted by any hardware.

Whenever a bug is 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.

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 61 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 600P
- SOHO 250
- SOHO 250W
- SOHO
- TZ
- TLS 1.1
- TLS 1.2
- IPSEC
- Firewall
- TCP
- UDP
- IPv4
- IPv6
- ICMPv4
- ICMPv6
- VPNGW
- VPN
- IPS
- Cavium Octeon III CN7020-800
- Cavium Octeon III CN7130-1400
- Cavium Octeon
- Cavium Octeon III CN7130-800
- Cavium Octeon III CN7130-1000
- Cavium Octeon III CN7130-1600
- Cavium Octeon II CN6635-800
- Cavium Octeon II CN6640-1100
- Cavium Octeon II CN6645-1200
- Cavium Octeon II CN6645-1300
- Cavium Octeon II CN6645-1500
- Cavium Octeon II CN6870-1000

- Cavium Octeon II CN6870-1200
- Cavium Octeon II CN6880-1400
- Cavium Octeon II CN6870-1000
- Cavium Octeon II CN6880-1200
- TZ 300
- TZ300W
- TZ400
- TZ400W
- TZ500
- TZ500W
- TZ600
- NSa 2650
- NSA 3600
- NSa 3650
- NSA 4600
- NSa 4650
- NSA 5600
- NSa 5650
- NSA 6600
- NSa 6650
- NSa 9250
- NSa 9450
- NSa 9650
- SM 9200
- SM 9400
- SM 9600
- SM 9800

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 8/11/2021. A follow up vulnerability scan was conducted on 9/27/2021. No vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

In review of the addition of new TOE HW, none of the changes impacts the evaluated functionality. The product properly maintained conformance to the protection profile while adding the new models. No changes made to the product across revisions impacts the functionality claimed within the original Security Target.

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 new hardware models,

shown above. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.