CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT
ASSURANCE CONTINUITY MAINTENANCE REPORT FOR:

AirTight Networks SpectraGuard Enterprise Version 7

Maintenance Report Number: CCEVS-VR-VID10441-2014

Date of Activity: 23 December 2014

References: Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004;

Impact Analysis Report for
AirTight Networks SpectraGuard Enterprise Version 7.0

Documentation Updated: (List all documentation updated)

- Security Target: ST
- Design Documentation: No changes required.
- Test Plan: Identify the new hardware that was tested.
- Lifecycle: No changes required
- Vulnerability Analysis: No changes required.
- Administrative Guidance: AGD

Assurance Continuity Maintenance Report:

The vendor for the AirTight Networks SpectraGuard Enterprise Version 7.0 submitted an Impact Analysis Report (IAR) to CCEVS for approval in December 2014. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 1.0, February 2004. 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 Target of Evaluation (TOE) is the AirTight Networks SpectraGuard Enterprise Version 7.0.

The TOE's third party software has been updated:

- The OpenSSL component of the TOE has been upgraded from the 2010 FIPS validated version 0.9.7d with FIPS object module 1.2 to the latest release 1.0.1g with FIPS object module 2.0.5 which is a version where the Heartbleed bug has been addressed. This assures that all security vulnerabilities in OpenSSL have been addressed. This is a minor change, as otherwise the usage of OpenSSL has not changed.

- The OpenSSH component of the TOE has been upgraded from version 5.3p1 to 6.5p1, which addresses all known security vulnerabilities to date in OpenSSH. This is a minor change, as otherwise the usage of OpenSSH has not changed.
- The CentOS component of the TOE has been upgraded from version 5.2 to 6.5, with a kernel version change from 2.6.18-92 to 2.6.32-431, as per customer requests.
- For the Sensor component of the TOE, the Linux subcomponent has been upgraded from 2.6.15 to 2.6.31.
- The PostgreSQL database component of the TOE has been upgraded from version 8.1.1 to 9.2.1.
- The SNMP component of the TOE has been upgraded from version 5.4.2.1 to 5.5.49.
- The libESMTP component of the TOE has been upgraded from version 1.0.4 to 1.0.6.
- The OpenLDAP component of the TOE has been upgraded from version 2.4.21 to 2.4.36.
- The server side (Servlet) Java Runtime Environment (JRE) changed from 1.6u13 to 1.7u51.

The following Table list specific changes to the TOE:

Type	Title and Synopsis	Assessment	Security Relevance
Enhancement	**OpenSSL Vulnerabilities** OpenSSL Heartbleed vulnerability (CVE-2014-0160) and SSL/TLS Man in the Middle attack (CVE-2014-0224)	These updates do not affect the cryptographic libraries of OpenSSL per se, but do affect how they are used by other components within OpenSSL.	Minor
Enhancement	ICMP timestamps are blocked from the SpectaGuard Enterprise server to the external hosts to enhance security of the system.	This reduces traffic that can be potentially analyzed by external entities.	Minor
Enhancement	Wireless client type information (smart device/smart device type) is now displayed whenever known. Setting added in Intrusion Prevention Policy to quarantine devices based on this information.	This is an auditing refinement on information already collected. This is an added quarantine mechanism.	None Minor
Enhancement Bug	**Device quarantine-related issues:** • Deauthentication-based quarantine is initiated for WPA2-PSK-encrypted ad hoc connections when they did not respond to cell splitting. • Sensor failed to prevent a quarantine-pending device after the troubleshooting session is stopped on that Sensor. This is fixed.	This augmentation of the quarantine capability is a functionality issue versus the security of the TOE. This is a correction to a functionality issue versus the security of the TOE.	Minor Minor
Enhancement Enhancement	**Device deletion-related issues:** • Added a link to delete all inactive Authorized Access Points (APs) in one operation. • Added support for deletion of individual BSSIDs within merged AP without having to split the merged entry.	This is an ease-of-use change that refines existing functionality. This is an ease-of-use change that refines existing functionality.	None None
Bug	Deauthentication technique made default instead of ARP poisoning for Multipot (multiple simultaneous honeypot APs).	This is a change in the default TOE configuration (the functionality used is different, but both capabilities already exist).	Minor
Enhancement Enhancement	**Marker packet-related issues:** • Stopped needless transmission of marker packets after NAT AP was detected as wired (network connected). • Marker packet transmission to clients disabled by default as service disruption was sometimes reported for clients connected to Cisco APs, due to transmission of these packets.	This reduces traffic that can be potentially analyzed by external entities. This prevents an inadvertent DOS situation.	Minor Minor

Type	Title and Synopsis	Assessment	Security Relevance
Enhancement	Configuration setting is introduced to not raise "Honeypot/Evil Twin active" event for Guest SSIDs.	This is a change to allow this event to be raised or not raised. The functionality already exists.	None
Enhancement	Channels for Sensor operation are updated taking into account the information/feedback for various regulatory domains in the world.	This is self-explanatory.	Minor
Bug	Transient Misconfigured AP events would occasionally be raised on newly-detected APs. This issue is now fixed.	This is a logic error on captured data.	Minor
Bug	"Turn off vulnerability status for event" and "Mark event for deletion" operations in the security scorecard used to cause a server crash. This is fixed.	This prevents an inadvertent DOS situation.	Minor
Bug	Sensor used to report an empty string for the gateway MAC address of a detected AP, causing a non-wired AP to be classified as a wired device in certain situations. This bug is fixed.	This is a logic error on captured data.	Minor

The TOE has no known outstanding security-related vulnerabilities at this time.

The vendor has done regression testing that has been reviewed by the CCTL.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found it to be minor. The ST is acceptable as the product was designed to meet FIPS 140-2 requirements.