Security Vulnerability Handling

For AudioCodes Session Border Controllers

This document provides security information for AudioCodes family of Mediant™ Session Border Controllers (SBC). This information is based on common industry practices, as well as on experience gained externally through certifications such as DoD FIPS, and through AudioCodes' continuous experience with internal vulnerability testing.

This information is kept up to date on a continual basis, adhering to industry trends and exposures to new vulnerabilities.

Security Approach for Critical Functional Areas

Functional Area	Security Measures in Use
Web Management via HTTPS	The SBC uses a proprietary Web server that is specifically hardened to provide tailored functionality. In other words, only minimum functionality required for the management of the SBC is kept active, while other features found in public open-source Web servers are removed. This reduces the attack surface of the SBC's Web server, eliminating many common security threats. The protection capability of the SBC's Web server is tested using an extensive third-party, test suite that covers generic vulnerabilities as well as potential attack insertion points.
Transport Layer Security (TLS) and Secure Sockets Layer (SSL)	Using OpenSSL as the TLS/SSL toolkit and cryptography library. The SBC uses the Long-term Support (LTS) stream of OpenSSL 1.0.2.
CLI (using SSH)	Access to the SBC through the Command Line Interface (CLI) can be configured to employ the following authentication methods: ▪ SSH key pairs ▪ Username-password combination ▪ Disable (no CLI access)
SNMP	Secure communication using SNMPv3.
Operating System (OS)	The SBC's OS is a highly-customized version of CentOS 6. The OS is “vertically” integrated with the application

AudioCodes Inc.
200 Cottontail Lane, Suite A101E
Somerset, NJ 08873
Tel: 1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
https://www.audiocodes.com/corporate/offices-worldwide
Website
https://www.audiocodes.com

Functional Area	Security Measures in Use
	(i.e., it is installed and updated as part of the application install or update). No third-party applications run concurrently with the SBC software (access to the OS is completely blocked). Only the necessary bare-minimum set of CentOS packages are installed. All standard services (including SSH, Telnet, NTP etc.) are replaced with home-grown implementation. Access to the Linux terminal is blocked (both from console and SSH/Telnet); instead, the application-level CLI is presented.

Proactive Vulnerabilities Tracking

AudioCodes actively searches for potential vulnerabilities on an on-going basis. It does this by employing the following methods:

Continues Open-Source (CVE) Threat Reports Analysis

Common Vulnerabilities and Exposures (CVE) reports for open source components (for example, OpenSSL, CentOS) are tracked and analyzed by AudioCodes on an ongoing basis. New reported CVEs are tracked and analyzed by R&D to determine the needed response on a case by case bases.

AudioCodes Security Quality Assurance

AudioCodes Quality Assurance team routinely tests the SBC with various security testing equipment such as: Symantec Nessus, IXIA, PROTOS, Spectra 2, ISIC, SipP, Burp Suite Professional.

AudioCodes One Voice™ Operation Center (OVOC), which includes the EMS and SEM applications, is regularly scanned using security scanning tools. These tools include Nessus® and Burp Suite Professional.

Above tests are performed as part of the AudioCodes software release process.

AudioCodes Inc.
200 Cottontail Lane, Suite A101E
Somerset, NJ 08873
Tel: 1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
https://www.audiocodes.com/corporate/offices-worldwide
Website
https://www.audiocodes.com

Third-Party Audits

AudioCodes SBCs (Mediant VE, Mediant 9000 and Mediant 4000) have been tested for performance, resiliency and security by Miercom (a third-party testing lab) and were proved fully resilient against DDoS attacks on both signaling and RTP/media ports. You can view the testing reports on the AudioCodes website:

https://www.audiocodes.com/library?query=Miercom

Addressing Potential Vulnerabilities

Potential vulnerabilities are handled using the following structured process:

1. Potential vulnerabilities are collected, as described above, from internal testing, external audits, and community reports.
2. The severity of each potential security vulnerability is determined and the potential threat it poses for users is analyzed. Specific care is taken to determine if a threat has an impact on the specific libraries in use and the functionality of the product.

   For threats determined as high risk, an immediate Product Notice is issued to AudioCodes partners and customers to alert of a critical security breach. The Product Notice includes information about the vulnerability, possible workarounds and a fix date.
3. A security update that fixes the vulnerability is released per the security patch release cadence described below.

AudioCodes Inc.
200 Cottontail Lane, Suite A101E
Somerset, NJ 08873
Tel: 1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
https://www.audiocodes.com/corporate/offices-worldwide
Website
https://www.audiocodes.com

Security Patch Release Cadence

AudioCodes releases a major software version every six months. Patch releases (mostly for bug fixes, security patches and small features) are released every two months. These releases include updates to various software components such as OpenSSL, CentOS and Web server, per security and functional requirements.

The following table describes the planned cadence of software updates:

Time Frame	Update Type	Update Content
Immediate	Response to a specific critical security threat	A Product Notice is issued to AudioCodes partners and customers including information and a target fix date.
Every two months	Patch release	Bug fixes and security patches for various software components such as OpenSSL, CentOS and Web server.
Every six months	Major software version release	Cumulative security updates and revision update of various software components such as OpenSSL, CentOS and Web server.

AudioCodes Inc.
200 Cottontail Lane, Suite A101E
Somerset, NJ 08873
Tel: 1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
https://www.audiocodes.com/corporate/offices-worldwide
Website
https://www.audiocodes.com