Security Vulnerability Handling

For AudioCodes Session Border Controllers, One Voice Operations Center (OVOC), AudioCodes Routing Manager (ARM) and IP Phones

This document provides security information for AudioCodes family of Mediant™ Session Border Controllers (SBC), One Voice Operations Center (OVOC) and IP Phones. 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 Main Critical Functional Areas

SBC

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 1.1.1.

Document #: LTRT-91108 Date: April, 2021

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
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 8 stream (SBC Version 7.4 and later). The OS is "vertically" integrated with the application (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.

OVOC

Functional Area	Security Measures in Use
Web Management via HTTPS	OVOC uses Apache Web server. The protection capability of the OVOC 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 OVOC uses the Long-term Support (LTS) stream of OpenSSL 1.0.2.
HTTPS	Secure communication using HTTPS.
SNMP	Secure communication using SNMPv3.
Operating System (OS)	The OVOC OS is a customized version of CentOS 7. The OS is integrated with the application, i.e., it is installed and updated as part of the application installation or update.

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
	No third-party applications run concurrently with the OVOC software. Only the necessary bare-minimum set of CentOS packages are installed.

ARM

Functional Area	Security Measures in Use
Web Management via HTTPS	ARM uses Apache Web server. The protection capability of the ARM 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)	OpenSSL is used as the TLS/SSL toolkit and cryptography library. The ARM uses OpenSSL 1.1.1.g FIPS. Java's Secure Socket Extension (JSSE) is used for Java-related TLS / SSL Communication. The ARM uses JSSE implementation of JDK 11.
HTTPS	Secure communication using HTTPS.
CLI (using SSH)	Access to the ARM through the Command Line Interface (CLI) using Username-password combination; root login is not allowed by default.
Operating System (OS)	The ARM OS is a customized version of CentOS 8. The OS is integrated with the application (i.e., it is installed and updated as part of the application install or update). No third-party applications run concurrently with the ARM software. Only the necessary bare-minimum set of CentOS packages are installed.

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

Native Teams IP Phones

Functional Area	Security Measures in Use
Web Management via HTTPS	The Native Teams IP phones do not use an embedded Web server for phone configuration. All the Web services are customized to connect to Office 365 services and to AudioCodes managed services such as the OVOC.
Sign in to Microsoft Teams	The Native Teams phone is signed in to Teams either with user credentials or using a special mode in which the user does not type the credentials but rather obtains a code from the phone (displayed on the screen) which is then used to sign in via the PC. In addition, IT can leverage MFA to further improve the security of the sign-in process.
Management from Device Manager	The IP phone supports management and provisioning by AudioCodes' Device Manager via HTTPS protocol. The phone validates the identity of the Device Manager using a known root CA.
Transport Layer Security (TLS)	BoringSSL is used to implement cryptography and TLS.
Android Debug Bridge (ADB)	AudioCodes disables the Android Debug Bridge (ADB) application and keeps the Teams app running in the front all the time, which means there is no way to install other Apps from unknown sources and sideloading.
CLI (using SSH)	The Native Teams phone leverages SSH as a debugging interface. AudioCodes recommends that customers disable SSH on the device. This can be done via AudioCodes' Device Manager (OVOC). SSH *must* be disabled by default and enabled only per specific case for debugging purposes only.
HTTPS	The phone uses HTTPS protocol for accessing Microsoft Teams admin center. This is enabled only after a successful secured sign-in process.
Operating System (OS)	The phone's OS is a customized version of Android (7.0 or 9.0 depending on the phone model) running in Android Kiosk mode. Only specific Microsoft apps and AudioCodes signed apps that were certified and approved in the certification process, can run under Kiosk mode.

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
App Signing	Android requires that all apps are digitally-signed with a developer key before installation; currently, the device verifies that the apps are signed by Microsoft.
Google play services	Goggle Play services were removed from the device software – no access is allowed to any Google store or Play services.
Device file system	The device file system is encrypted.
Android Security Updates	AudioCodes regularly adopts and integrates Android security updates.

Teams Compatible / Generic SIP IP Phones

Functional Area	Security Measures in Use
Web Management via HTTPS	IP phones optionally use an embedded proprietary Web server for phone configuration. For phone security hardening, it's recommended to disable the phone's Web server via configuration, or to limit it to a specific and preconfigured access list.
Management from Device Manager	The IP phone supports management and provisioning by the Device Manager via HTTPS protocol. The management interface can be restricted to use HTTPS only and limited to a specific access list.
Transport Layer Security (TLS) and Secure Sockets Layer (SSL)	OpenSSL is used as the TLS/SSL toolkit and cryptography library. The phones use the Long-Term Support (LTS) stream of OpenSSL 1.0.2.
CLI (using SSH)	Access to the phone 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) For security hardening, the Telnet management interface can be disabled and the CLI interface can be limited to a specific access list.

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
HTTPS	The phone uses HTTPS protocol for provisioning, management and for accessing Web services. HTTPS traffic uses TLS 1.2 transport. For TLS 1.2 connections, it's recommended to use one of the following advanced cipher suites: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
SIP	SIP Signaling protocol is used by the phone to establish voice sessions. All SIP traffic uses TLS 1.2 transport.
Operating System (OS)	The phone's OS is a highly-customized version of Embedded Linux. Only the necessary, bare-minimum set of Linux components and utilities are enabled.

Proactive Vulnerabilities Tracking

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

Continuous 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 basis.

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.

The 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 considered high risk, an immediate Product Notice is issued to AudioCodes partners and customers to alert to 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.

Document #: LTRT-91108 Date: April, 2021

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