AudioCodes
Security Vulnerability Handling

This document provides security information for the following AudioCodes products:

- Session Border Controllers (SBC)
- One Voice Operations Center (OVOC)
- AudioCodes Routing Manager (ARM)
- Native Teams IP Phones
- Teams Compatible and Generic SIP IP Phones
- Microsoft Teams Rooms (MTR) on Android

This information is based on common industry practices, as well as 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.

Document #: LTRT-91113
Date Published: Dec 2024

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Or Yehuda, 6032303,
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

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) 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.

Third-Party Security Scan and Penetration Test

AudioCodes has built long-term partnerships with third-party professional security testing organizations. Regular vulnerability scanning and penetration testing are conducted, initiated both by AudioCodes and upon the request of customers.

AudioCodes Security Quality Assurance

The AudioCodes Quality Assurance team regularly tests AudioCodes products (SBCs, OVOC, Devices, etc.) using various security testing tools, including Nessus®, Burp Suite Professional, IXIA, PROTOS, Spectra 2, ISIC, and SIPp. These tests are conducted as part of the AudioCodes software release process.

Document #: LTRT-91113
Date Published: Dec 2024

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Or Yehuda, 6032303,
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

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.

Document #: LTRT-91113
Date Published: Dec 2024

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Or Yehuda, 6032303,
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
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, OS 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, OS, and Web server.
Every six months	Major software version release	Cumulative security updates and revision update of various software components such as OpenSSL, OS and Web server.

Document #: LTRT-91113
Date Published: Dec 2024

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Or Yehuda, 6032303,
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

Security Approach for Main Critical Functional Areas

Session Border Controllers (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 1.1.1t.
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 Rocky Linux (SBC Version 7.4.500 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).

Document #: LTRT-91113
Date Published: Dec 2024

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Or Yehuda, 6032303,
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

Functional Area	Security Measures in Use
	No third-party applications run concurrently with the SBC software (access to the OS is completely blocked). Only the necessary bare-minimum set of OS 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.
OS Patching and Third-Party Applications Policy	AudioCodes provides all necessary OS patches as part of regular maintenance software updates, removing the need for separate OS patching. Additionally, there is no possibility of installing any third-party application on the SBC device. Any required patches for security vulnerabilities are provided by AudioCodes in accordance with our vulnerability handling procedure.

Document #: LTRT-91113
Date Published: Dec 2024

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Or Yehuda, 6032303,
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

OVOC (Ver. 8.4)

Functional Area	Security Measures in Use
Web Management via HTTPS	OVOC uses Apache Web server. The server is configured using the recommended security properties both by the Apache Tomcat documentation and by other security companies. The protection capability of the 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. OVOC uses the Long-term Support (LTS) stream of OpenSSL 1.1.1k version.
HTTPS	Secure communication using HTTPS (default).
SNMP	Secure communication using SNMPv3.
Operating System (OS)	The OVOC OS is a customized version of Rocky Linux (OVOC 8.4 and later). The OS is integrated with the application (i.e., installed and updated as part of the application installation or update). No third-party applications run concurrently with the OVOC software. Only the necessary bare-minimum set of Rocky Linux packages are installed.
OS Patching and Third-Party Applications Policy	AudioCodes provides all necessary OS patches as part of regular maintenance software updates, removing the need for separate OS patching. Additionally, there is no possibility of installing any third-party application on OVOC. Any required patches for security vulnerabilities are provided by AudioCodes in accordance with our vulnerability handling procedure.

Document #: LTRT-91113
Date Published: Dec 2024

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Or Yehuda, 6032303,
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

ARM (Ver. 10.0)

Functional Area	Security Measures in Use
Web Management via HTTPS	ARM uses the Apache Tomcat web server, LTS version 10.0.x. The server is configured using the recommended security properties both by the Apache Tomcat documentation and by other security companies. The protection capability of the 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. ARM uses Long-term Support (LTS) stream of OpenSSL, more specifically the 1.1.1.k version. Java's Secure Socket Extension (JSSE) is used for Java related TLS / SSL Communication (Web server and HTTP client). ARM uses JSSE implementation of JDK 17.
HTTPS	Secure communication using HTTPS (default).
CLI (using SSH)	Access to ARM through the Command Line Interface (CLI) using username-password combination; root login is not allowed by default. ARM uses OpenSSH version LTS 8.0.
Operating System (OS)	The ARM OS is a customized version of the Rocky Linux (ARM 10.0 and higher). The OS is integrated with the application (i.e., installed and updated as part of the application install or update). Only a small number of bare-minimum applications and packages that are required for ARM's operation are installed. No third-party applications run concurrently with the ARM software.

Document #: LTRT-91113
Date Published: Dec 2024

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Or Yehuda, 6032303,
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

Functional Area	Security Measures in Use
	These packages are regularly updated per ARM version.
OS Patching and Third-Party Applications Policy	AudioCodes provides all necessary OS patches as part of regular maintenance software updates, removing the need for separate OS patching. Additionally, there is no possibility of installing any third-party application on ARM. Any required patches for security vulnerabilities are provided by AudioCodes in accordance with our vulnerability handling procedure.

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)

Document #: LTRT-91113
Date Published: Dec 2024

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Or Yehuda, 6032303,
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

Functional Area	Security Measures in Use
	For security hardening, the Telnet management interface can be disabled and the CLI interface can be limited to a specific access list.
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.
OS Patching Policy	AudioCodes provides all necessary OS patches as part of regular maintenance software updates, removing the need for separate OS patching.

Document #: LTRT-91113
Date Published: Dec 2024

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Or Yehuda, 6032303,
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

Native Teams IP Phones

For security vulnerability handling of AudioCodes Native Teams IP Phones, please refer to Security Guidelines for AudioCodes' Android-based Devices and Generic SIP Phones.

Microsoft Teams Rooms (MTR) on Android

For security vulnerability handling of Microsoft Teams Rooms (MTR) on Android devices, please refer to Security Guidelines for AudioCodes' Android-based Devices and Generic SIP Phones.

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Or Yehuda, 6032303,
P.O. Box 255, Ben Gurion Airport, Israel, 70100
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com