



Vulnerabilities in PHP Affecting AudioCodes Products

Product Notice #0600

Severity: Critical
First Published: 2026 October 22
Version 1.0: Interim

Summary

- On October 21, 2026, the PHP Foundation announced the availability of a Critical PHP security release that addresses the following vulnerabilities:
 - ✓ [CVE-2026-109618](#): Remote code execution via out-of-memory (OOM) corruption
 - ✓ [CVE-2026-109619](#): Remote code execution via stale global state
- For a description of these vulnerabilities, see the [PHP Foundation announcement](#) and the GitHub security advisories linked above.
- The vast majority of AudioCodes products are not affected.** This includes the widely deployed AudioCodes Mediant Session Border Controllers (SBCs), Voice over IP (VoIP) Gateways, IP Phones and Meeting Space devices which do not use PHP.
- Real-time services, including voice calls and bot interactions, are not impacted.** Where an AudioCodes product is affected, the exposure is limited to its PHP-based web or management components.
- AudioCodes-hosted services are protected.** AudioCodes has deployed updated Web Application Firewall (WAF) protections across its hosted infrastructure, including AudioCodes Live Platform, and is deploying fixed software. Customers using these services do not need to take any action.
- AudioCodes began releasing fixed software for affected products, starting with AudioCodes-hosted services.
- This advisory will be updated as additional information becomes available.

Affected Products

AudioCodes has confirmed that the following products are affected by the vulnerabilities that are described in this advisory.

- Voice and Unified Communications**
 - ✓ AudioCodes Survivable Branch Appliance (SBA)
 - ✓ AudioCodes Fax Server
- Contact Center**
 - ✓ AudioCodes VOCA CIC (customer-hosted)
- Network Management**
 - ✓ AudioCodes Device Manager
- AudioCodes Cloud Hosted Services**
 - ✓ AudioCodes Live Platform
 - ✓ AudioCodes VOCA CIC (AudioCodes cloud)

AudioCodes has confirmed that these vulnerabilities do not affect any AudioCodes products other than those listed above.

This section may be updated as information becomes available.

AudioCodes Response

Upon disclosure of these vulnerabilities, AudioCodes took the following proactive measures to protect its customers and hosted services while fixed software is being deployed:

- Updated Web Application Firewall (WAF) protections across AudioCodes-hosted infrastructure to block exploitation attempts targeting these PHP vulnerabilities.
- Engaged its security operations center to apply heightened monitoring of traffic toward AudioCodes products and hosted services.
- AudioCodes began releasing fixed software for affected products, starting with AudioCodes-hosted services

Customers who host affected products in their own environment should upgrade as soon as fixed software is available.

Revision History

Version	Description	Status	Date
1.0	Initial public release.	Interim	2026 October 22

Legal Disclaimer

Software Downloads and Technical Support

Customers with a valid support agreement should obtain fixed software through their regular update channels. Customers without a support agreement, or who need assistance, should contact AudioCodes Technical Support.

Legal Disclaimer Details

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. AUDIOCODES RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.



If you have any questions, contact us at
www.audiocodes.com/corporate/offices-worldwide

AudioCodes Ltd. | Naimi Park, 6 Ofra Haza Street | Or Yehuda | Israel | +972-3-976-4000