IP オーディオシリーズにおける PHP をはじめとする複数の脆弱性

公開日：2026 年 11 月 04 日

最終更新日：2026 年 11 月 04 日

TOA 株式会社

■脆弱性情報　ID

TV2026-001

■概要

IP　オーディオシリーズにおいて、オープンソースのスクリプト言語「PHP」におけるリモートコード実行の脆弱性をはじめとする複数の脆弱性を確認しました。これらの脆弱性により、悪意ある第三者によって、任意のコードがリモートで実行される可能性や、製品を不正に操作される、または情報を不正に取得される可能性があります。

現時点では、当社製品に対してこれらの脆弱性を悪用した攻撃の発生は確認されておりませんが、より安心してご使用いただくため、該当製品をご使用中のお客様は修正済みファームウェアへアップデートしていただきますようお願いいたします。

■該当製品の確認方法

影響を受ける製品は以下の通りです。

製品名	品番	対象のファームウェアバージョン
IP 音声インターフェース	IP-A1AF	Ver.3.6.1 以前の全て
IP 小型アンプ　12W	IP-A1PA12	Ver.3.6.1 以前の全て
IP 天井埋込型スピーカー　8W	IP-A1PC238	Ver.3.6.1 以前の全て
IP ページングゲートウェイ	IP-A1PG	Ver.3.6.1 以前の全て
IP リモートマイク	IP-A1RM	Ver.3.6.1 以前の全て
IP ホーンスピーカー　15W	IP-A1SC15	Ver.3.6.1 以前の全て

＜バージョン確認方法＞

現在ご使用中のファームウェアのバージョン情報を確認する方法は、受信端末設定説明書または送信端末設定説明書に記載しております。当社商品データ ダウンロードサイトから品番を検索いただき、ご確認ください。

商品データ ダウンロードサイト

https://www.toa-products.com/download/

■脆弱性の説明

これらの脆弱性は、該当製品とネットワークで通信できる第三者によって悪用される可能性があります。

脆弱性種別 または識別番号	脆弱性内容	CVSS スコア
CVE-2026-109618	PHP におけるメモリ不足時の処理の不備 (リモートコード実行のおそれ)	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N 基本値：9.2 (外部機関による公開情報)
CVE-2026-109619	PHP における解放済みメモリの使用 (リモートコード実行のおそれ)	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N 基本値：9.2 (外部機関による公開情報)
CWE-306	重要な機能に対する認証の欠如	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値：9.8 (自社評価)
CWE-78	OS コマンドインジェクション	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値：8.1 (自社評価)
CWE-338	暗号における脆弱な PRNG の使用	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H 基本値：7.7 (自社評価)
CWE-287	不適切な認証	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値：9.8 (自社評価)
CWE-294	Capture-replay による認証回避	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H 基本値：7.7 (自社評価)
CWE-862	認可の欠如	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H 基本値：8.1 (自社評価)

■対策方法

本脆弱性に対する対策として、該当製品に対して、脆弱性を修正したファームウェアをご提供しております。

当社商品データダウンロードサイトから品番を検索して修正済みファームウェアをダウンロードいただき、アップデートを実施してください。

ファームウェアのアップデート方法は、受信端末設定説明書または送信端末設定説明書に記載しております。

なお、修正済みファームウェアにアップデートした後は、それより前のバージョンに戻すことはできません。

商品データ ダウンロードサイト

https://www.toa-products.com/download/

修正済みファームウェア

Ver.3.6.2 以降

■一時的なリスク軽減策

すぐに修正済みファームウェアへのアップデートを実施できない場合は、次の対策により一時的にリスクを軽減できます。

・インターネットから直接アクセスできないネットワークで使用する

・ファイアウォールやルーターなどにより、該当製品と通信できる機器を限定する

・該当製品との通信には、HTTPS を使用する

一時的な措置となります。アップデートを実施できる状況になりましたら、修正済みファームウェアへアップデートしていただきますようお願いいたします。

■お問い合わせ窓口

本件に関するお問い合わせは、当社の各営業所にて承っております。

最寄りの当社営業所までお問い合わせください。

https://www.toa-global.com/ja/profile/company/network

■更新履歴

2026 年 11 月 04 日

この脆弱性情報を公開しました。