PHP and Other Vulnerabilities in the IP-A1 Series

Published : November 04, 2026

Last Updated : November 04, 2026

TOA Corporation

■Security Advisory ID

TV2026-002

■Overview

Multiple vulnerabilities, including a remote code execution vulnerability in PHP, exist in the IP-A1 Series. These vulnerabilities may allow a malicious third party to remotely execute arbitrary code, perform unauthorized operations on the product, or obtain information without authorization.

At the time of publication, we are not aware of any exploitation of these vulnerabilities against our products. However, to ensure continued secure operation, customers using affected products are recommended to update to the fixed firmware versions.

■Affected products

The affected products and versions are as follows.

Product name	Model Number	Affected Firmware Versions
IP Audio Interface	IP-A1AF	Ver.3.6.1 and prior
IP Power Amplifier 12W	IP-A1PA12	Ver.3.6.1 and prior
IP Ceiling Speaker 8W	IP-A1PC238	Ver.3.6.1 and prior
IP Paging Gateway	IP-A1PG	Ver.3.6.1 and prior
IP Remote Microphone	IP-A1RM　Y	Ver.3.6.1 and prior
IP Horn Speaker 15W	IP-A1SC15	Ver.3.6.1 and prior
IP Ceiling Mount Speaker	IP-A1PC580R	Ver.3.6.1 and prior
IP Square Speaker 8W	IP-A1PC580S	Ver.3.6.1 and prior

＜How to Check the Versions＞

For detailed instructions on how to check the version, please refer to the applicable setup manual (RECEIVING DEVICE SETUP MANUAL or TRANSMITTING DEVICE SETUP MANUAL). The manuals are available from the Products Data Download Site below. Please search for your product model number to find the appropriate manual.

Products Data Download Site

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

■Description

These vulnerabilities may be exploited by a third party who can communicate with the affected products over the network.

CVE ID or CWE	Description of the vulnerabilities	CVSS Score
CVE-2026-109618	Improper Handling of Out-of-Memory Conditions in PHP (Potential Remote Code Execution)	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 CVSS-B : 9.2 (Public information)
CVE-2026-109619	Use After Free in PHP (Potential Remote Code Execution)	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 CVSS-B : 9.2 (Public information)
CWE-306	Missing Authentication for Critical Function	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score : 9.8 (Vendor Assessment)
CWE-78	OS Command Injection	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score : 8.1 (Vendor Assessment)
CWE-338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H Base Score : 7.7 (Vendor Assessment)
CWE-287	Improper Authentication	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score : 9.8 (Vendor Assessment)
CWE-294	Authentication Bypass by Capture-replay	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H Base Score : 7.7 (Vendor Assessment)
CWE-862	Missing Authorization	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H Base Score : 8.1 (Vendor Assessment)

■Countermeasures for Customers

Fixed firmware versions are available for the affected products.

Please download the fixed firmware version from the following website and update your product accordingly.

Products Data Download Site

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

＜Fixed Firmware Version＞
Ver.3.6.2 or later

＜How to Update the Firmware＞
For instructions on how to update the firmware, please refer to the applicable setup manual (RECEIVING DEVICE SETUP MANUAL or TRANSMITTING DEVICE SETUP MANUAL).
Please note that after updating to the fixed firmware, you cannot return to an earlier version.

■Temporary Risk Mitigation
If you cannot update to the fixed firmware immediately, the following measures can temporarily reduce the risk.
• Use the products on a network that cannot be accessed directly from the Internet.
• Restrict the devices that can communicate with the products by using a firewall, router, etc.
• Use HTTPS for communication with the products.
These are temporary measures. Once you are able to update, please update to the fixed firmware.

■Contact information
Please contact your local TOA representative.
https://www.toa-global.com/en/profile/company/network

■Update history
November 04, 2026
Published