

Security Advisory – Vulnerability found in EZ-P21

Advisory ID	SA-202608-001
Release Date	Aug-26
Product	CP PLUS EZ-P21 Camera
Severity	High
Update Type	Over-The-Air (OTA) Firmware Security Update

Summary

CP PLUS has released a new firmware version for the EZ-P21 IP Camera that addresses multiple security vulnerabilities identified through responsible security research. These vulnerabilities could potentially allow unauthorized access to device functionality and camera data under specific conditions.

Customers are strongly advised to install the latest firmware through the Over-The-Air (OTA) update mechanism to ensure continued security and protection of their devices

Affected Products

Product	EZ-P21
Affected Firmware Version(s)	V4.8.8.1
Fixed Firmware Version	V4.8.16.1

Vulnerabilities Addressed

1. Arbitrary Code Execution via SD Card

Severity: High

A security issue was identified in the device startup process that could allow execution of unauthorized code from removable storage under specific circumstances involving physical access to the device. The updated firmware removes the insecure behavior and introduces additional validation controls to prevent unauthorized executable content from being loaded.

Security enhancements implemented:

- Removal of insecure debug functionality from production firmware
- Enhanced executable validation mechanisms
- Improved startup security controls
- Additional restrictions on externally supplied binaries

2. Unauthorized Access to Snapshot and Video Endpoints

Severity: High

A vulnerability affecting authentication controls could allow unauthorized access to camera snapshots and streaming-related functionality. The updated firmware strengthens authentication enforcement and hardens access control mechanisms for web-accessible services.

Security enhancements implemented:

- Strengthened authentication validation
- Enforcement of secure credential requirements
- Improved access control for camera resources
- Enhanced protection against unauthorized access attempts
- Additional service hardening measures

Recommended Actions

All customers should immediately:

- a. Connect the camera to the internet.
- b. Check for available OTA firmware updates.
- c. Install the latest firmware version.
- d. Verify that the device is running the updated firmware.
- e. Review device credentials and ensure strong passwords are configured.

Successful installation of the latest OTA firmware fully addresses the reported vulnerabilities affecting:

- Unauthorized code execution risks
- Unauthorized snapshot access
- Unauthorized video stream access
- Weak authentication handling

The update also includes additional security hardening and stability improvements.

Acknowledgements

CP PLUS appreciates the efforts of security researcher Mr. Deven Lunkad, Indian Institute of Information Technology, Allahabad, who responsibly disclosed these findings and helped improve the security of our products.

Support

Customers requiring assistance with the firmware update process should contact CP PLUS Technical Support through official support channels.

In line with cybersecurity best practices, we strongly recommend that all CP PLUS customers follow our security advisories to ensure product systems are up to date and customers' rights are fully protected. If you have additional concerns regarding cybersecurity-related issues, please contact us at support@cpplusworld.com

Revision History

Version	Description	Date
V1.0	Initial public release	10th August 2026