

# Forum:[Hack Forums](#)

Thread: [Apeman Cameras](#)

Stanley - March 22, 2026, 5:35 am

Apeman Cameras

View CSAF

Summary

Successful exploitation of these vulnerabilities could allow an attacker to take control of the device or view camera feeds.

The following versions of Apeman Cameras are affected:

ID71 vers:all/\* (CVE-2025-11126, CVE-2025-11851, CVE-2025-11852)

CVSS

Vendor

Equipment

Vulnerabilities

v3 9.8

Apeman

Apeman Cameras

Insufficiently Protected Credentials, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Missing Authentication for Critical Function

Background

Critical Infrastructure Sectors: Commercial Facilities

Countries/Areas Deployed: Worldwide

Company Headquarters Location: China

Vulnerabilities

Expand All +

CVE-2025-11126

A security flaw has been discovered in Apeman ID71 218.53.203.117. This vulnerability affects

unknown code of the file /system/www/system.ini. The attack may be performed from remote. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.

[View CVE Details](#)

#### Affected Products

Apeman Cameras

Vendor:Apeman

Product Version:Apeman ID71: vers:all/\*

Product Status:known\_affected

#### Remediations

MitigationApeman did not respond to CISAs request for coordination. Users are encouraged to reach out to Apeman for support <https://apemans.com/pages/contactus>

Relevant CWE: CWE-522 Insufficiently Protected Credentials

#### Metrics

#### CVSS Version

Base Score

Base Severity

Vector String

3.1

9.8

CRITICAL

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

#### CVE-2025-11851

A vulnerability has been found in Apeman ID71 EN75.8.53.20. The affected element is an unknown function of the file /set\_alias.cgi. Such manipulation of the argument alias leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.

[View CVE Details](#)

#### Affected Products

Apeman Cameras

Vendor:Apeman  
Product Version:Apeman ID71: vers:all/\*  
Product Status:known\_affected

#### Remediations

MitigationApeman did not respond to CISAs request for coordination. Users are encouraged to reach out to Apeman for support <https://apemans.com/pages/contactus>

Relevant CWE: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

#### Metrics

CVSS Version  
Base Score  
Base Severity  
Vector String

3.1  
3.5  
LOW  
CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N

#### CVE-2025-11852

A vulnerability was found in Apeman ID71 218.53.203.117. The impacted element is an unknown function of the file /onvif/device\_service of the component ONVIF Service. Performing manipulation results in missing authentication. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.

[View CVE Details](#)

Affected Products  
Apeman Cameras

Vendor:Apeman  
Product Version:Apeman ID71: vers:all/\*  
Product Status:known\_affected

## Remediations

MitigationApeman did not respond to CISAs request for coordination. Users are encouraged to reach out to Apeman for support <https://apemans.com/pages/contactus>

Relevant CWE: CWE-306 Missing Authentication for Critical Function

## Metrics

### CVSS Version

Base Score

Base Severity

Vector String

3.1

5.3

MEDIUM

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

## Acknowledgments

CISA discovered the PoCs (Proof of Concept) as authored by Julio Urena

## Legal Notice and Terms of Use

This product is provided subject to this Notification (<https://www.cisa.gov/notification>) and this Privacy & Use policy (<https://www.cisa.gov/privacy-policy>).

## Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities, such as:

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on [cisa.gov/ics](https://cisa.gov/ics). Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at [cisa.gov/ics](https://cisa.gov/ics) in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

Do not click web links or open attachments in unsolicited email messages.

Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

No known public exploitation specifically targeting these vulnerabilities has been reported to CISA at this time.

## Revision History

Initial Release Date: 2026-03-10

| Date | Revision | Summary |
|------|----------|---------|
|------|----------|---------|

|            |  |  |
|------------|--|--|
| 2026-03-10 |  |  |
|------------|--|--|

|   |  |  |
|---|--|--|
| 1 |  |  |
|---|--|--|

|                     |  |  |
|---------------------|--|--|
| Initial Publication |  |  |
|---------------------|--|--|

## Legal Notice and Terms of Use

<https://www.cisa.gov/news-events/ics-advisories/icsa-26-069-01>