CVE-2026-53986: Hardcoded TURN Credentials and Cleartext STUN/TURN Authentication in Girafit Camera App and Devices

The most popular home security camera on TikTok Shop ships its relay credentials in cleartext

Updated October 21, 2026 · 4 min read · Markdown

Jordan

CVE	CVE-2026-53986
Product	Girafit camera app (Android and iOS) and Girafit camera devices
Affected version	1.9.1 and earlier

Contents

Weaknesses	CWE-798: Use of Hard-coded Credentials; CWE-319: Cleartext Transmission of Sensitive Information
CNA	VulnCheck
Reported	June 2026
Disclosed	October 10, 2026
Fix status	Unknown. The vendor never responded to coordination

TL;DR

Girafit's camera app ships a static TURN username hardcoded in its code, identical for every install, and sends that username and a session token over the network unencrypted. Anyone who decompiles the app or watches its traffic gets both. The relay password was not exposed, so this does not grant relay access by itself.

Background

When you open a camera's live feed from your phone, the two devices usually sit behind different home routers that won't accept unsolicited inbound connections. STUN lets each side discover its public address so they can try to connect directly. When that fails, TURN (Traversal Using Relays around NAT) relays the video through a server in the middle. Because a relay forwards traffic for whoever is authenticated, TURN

servers require credentials. Without them, anyone could route their traffic through the vendor's infrastructure on the vendor's bill.

Discovery

I got into this after reading Sammy Azdoufal's writeup, Nobody Puts Baby in a Corner, and wanted to try the same kind of research on another IoT device. The candidate was obvious: a couple of weeks earlier, my older sister had eagerly shown me a "cheap but decent" camera with a "creepy voice." Girafit, as seen on Amazon and TikTok Shop. So I bought one.

I decompiled the Android APK with jadx and found the TURN server address and username stored as plain string literals in the app's Java code. I then captured the app's traffic with Wireshark while opening a live view and found the username and a session token transmitted in cleartext.

Technical Details

1. Hardcoded username (CWE-798)

The TURN server address and username are hardcoded as string literals in the Android app’s Java code.

The username is static, identical for every install, and not tied to any user account or device.

2. Cleartext transmission (CWE-319)

When the app opens a live view and registers the device, the username and a session token are sent unencrypted in the app’s network traffic.

Anyone positioned on the same network as the phone or camera can read both off the wire without touching the app.

Impact

- **Shared identity across every install:** because every copy of the app uses the same username, the relay can't distinguish one customer from another, or from anyone else who pulls the string out of the APK. It also can't be revoked for one user without breaking every user.
- **Session token exposed in transit:** the token crosses the network in cleartext, so it can be captured by anyone on the same Wi-Fi as the phone or camera.
- **Half of the credential pair is public:** relay access now depends entirely on the password staying secret.

What I Didn't Test

- **The relay password.** I didn't recover it, so I couldn't authenticate to the relay. Whether it's also static, or recoverable from the camera firmware, is open.
- **What the session token authorizes.** I didn't test whether a captured token can be replayed against Girafit's API or used to reach an account or camera.

Either one would raise the severity considerably and is worth a follow-up.

Disclosure Timeline

- **May 28th, 2026:** Reported to VulnCheck. CVE-2026-53986 provisionally allocated.
- **June 12th, 2026:** VulnCheck contacted Girafit. Girafit deadline set for September 24th.
- **June 30, 2026:** June 30, 2026: Girafit released version 1.9.4. Whether it addresses this issue is unconfirmed.

- **September 23, 2026:** The original September 24 disclosure deadline was extended to October 10 after my VulnCheck case contact changed.
- **October 10, 2026:** Public disclosure.

Remediation

For Girafit:

- Stop shipping static credentials. Issue short-lived, per-session TURN credentials from the backend after the user authenticates. The standard approach is time-limited HMAC credentials, supported by coturn and most TURN servers.
- Send the session token and any credential-bearing traffic over TLS, and use TURNS (TURN over TLS) for the relay itself.
- Rotate the current username and invalidate existing session tokens, since both should be considered public.

For users: there's no setting that fixes this. Keep the app and camera firmware updated in case a fix ships.

Credits

Discovered by Jordan Gaskin. Coordinated by VulnCheck, which assigned CVE-2026-53986.

29 views

About the author



Jordan

esteemed amateur

Comments

Join the discussion

No comments yet. Be the first to comment.

© 2026 Macrodata Refinement