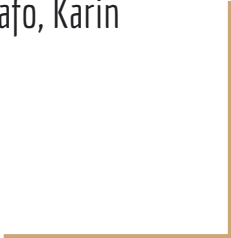


# EC521 Cybersecurity Project (Team 1)

Abdulaziz AlMailam, Kwadwo Osafo, Karin  
Luna



# Objective

- Evaluate IP Camera security using the Amcrest IP8M-2796EW-AI camera
- Cameras are used to secure property – ironically insecure
- Raise awareness about the various vulnerabilities within IP cameras
- Demonstrate common attacks:
  - a. Stack-based buffer overflow
  - b. Brute-force login
  - c. Denial-of-Service (DoS)



# Importance

- CCTV is the go-to source for visual evidence (crashed camera = no proof)
- Assumption of security & privacy when purchasing a camera
- More issues will arise as cameras become more advanced (i.e., Facial Recognition, Smart Alerts)
- An attack on one camera likely works on another, too
  - Dahua & Hikvision manufacture most of the world's cameras (i.e., Lorex, ICREALTIME, Amcrest, Bosch)



Search results for "Dahua" on Shodan

# Inspiration

- Past breaches and exposed security vulnerabilities
- Intrigue on progress made in the industry since
- Fictional depictions of it (Ocean's 8)

Ars Technica

## Eufy's "local storage" cameras can be streamed from anywhere, unencrypted

(Update 7:30 a.m. ET 12/2/2022: Eufy has issued a statement in response to findings from The Verge and a security researcher:.

Dec 1, 2022



CNET

## Eufy Cameras Caught Sending Local-Only Data to Cloud Servers

The camera manufacturer apparently did it without user knowledge, even when cloud storage was disabled.

Nov 29, 2022



Gizmodo

## Eufy Admits 'Local' Cameras Were Sending Unencrypted Streams

The security camera company's parent Anker promised all video stream requests will be E2E encrypted, and that every Eufy camera will be...

1 month ago



## Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals

- Hacker group says it wanted to show prevalence of surveillance
- Video footage was captured from Sequoia-backed startup Verkada

# Technical Approach

1. Reconnaissance and application fingerprinting
  - a. Packet capture & sniffing, port scanning
  - b. Identify exposed endpoints
  - c. Review source files
2. Review previous attacks and known vulnerabilities
3. Recreate previous attacks on different ports and protocols
  - a. Stack-based buffer overflow (i.e., TCP port)
  - b. Null pointer reference
  - c. Brute-force login script on non-rate-limited ports
  - d. Forge authentication handshakes (i.e., ONVIF protocol)

# Technical Approach (continued)

## 4. Impersonate storage locations

- a. Fraudulent FTP server, logging authentication credentials (credentials hard-coded at setup)
- b. NAS server, similar approach

## 5. Denial of Service (DoS) Attacks

- a. Too many concurrent authentication attempts
- b. Ping flooding, etc.

# Intermediary Results

The image displays a web browser window showing the AMCREST IP Camera Web Access interface. The interface includes a login form with fields for username (admin) and password, and a 'Login' button. Below the login form, there is a section for 'IP Camera Web Access' with a list of cameras and their status.

The browser's developer tools are open, showing the 'Sources' panel with a list of JavaScript files. The 'Console' panel is also open, displaying a JavaScript error: 'Uncaught ReferenceError: alert is not defined'.

Below the browser window, a network traffic analysis tool (Wireshark) is shown, displaying a list of network packets. The packets are captured on the 'eth0' interface and are of type 'HTTP'. The packets are numbered 1 through 49, and they show various HTTP requests and responses, including GET, POST, and PUT methods. The packets are captured from the source IP 192.168.1.108 to the destination IP 192.168.1.108.

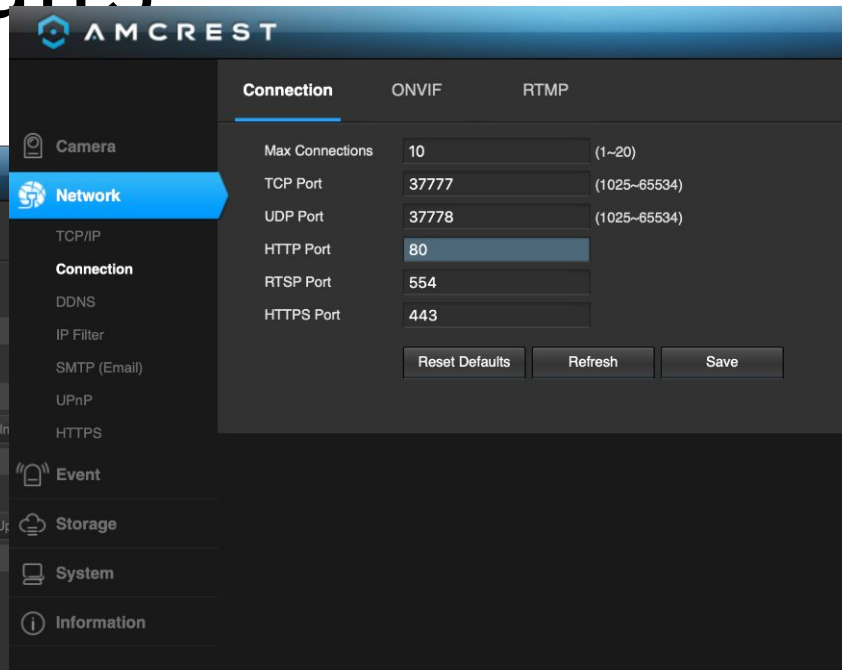
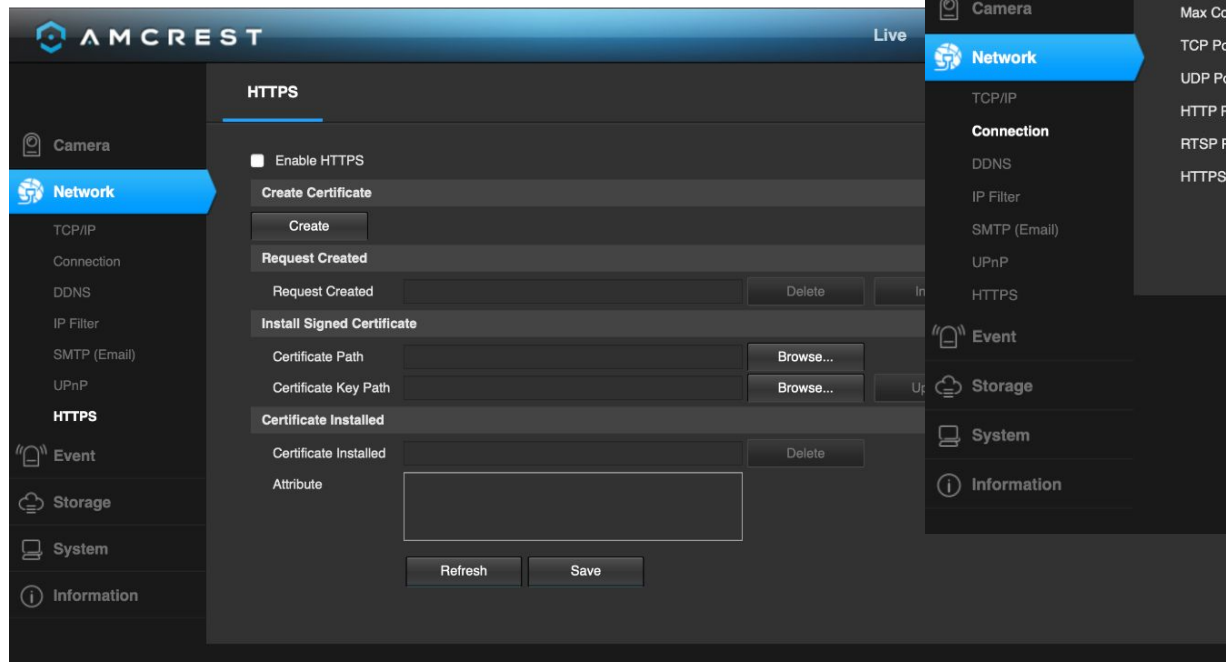
The Wireshark interface shows the following details for the selected packet (Packet 49):

- Frame 49: 1440 bytes captured on interface eth0, 1440 bytes captured (100.0%) on interface eth0
- Ethernet II, Src: AmcrestT\_3e:41:dc (9c:8e:cd:3e:41:dc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Discover)

The Wireshark interface also shows the packet's payload, which is a JSON object containing the following data:

```
{
  "type": "discovery",
  "data": {
    "ip": "192.168.1.108",
    "port": 68,
    "protocol": "HTTP",
    "method": "GET",
    "url": "/api/v1/discovery",
    "headers": {
      "Host": "192.168.1.108",
      "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36"
    },
    "body": ""
  }
}
```

# Intermediary Results





# Related Results

- Vulnerabilities known since first Amcrest/Dahua cameras release
- CVE-2020-5735, CVE-2020-5736 – [Tenable Proof of Concept \(2020\)](#)
- [Eufy Cameras Advertised as 'Local-Only' stored data on AWS servers](#)

Note: Updated firmware seems to only be provided on demand, so potentially the majority of devices could still possess these vulnerabilities