Independent Tests of
Anti-Virus Software


# IP Camera Test 2020

## Commissioned by PC Magazin

TEST PERIOD: MAY 2020
LANGUAGE: ENGLISH
LAST REVISION: 3. JUNE 2020

WWW.AV-COMPARATIVES.ORG

# Content

# Introduction

On behalf of PC Magazin, we examined the security aspects of six home security-camera systems. PC Magazin specified the devices to be tested, the test methods, and the test criteria for evaluating the camera systems. However, we added some additional security-related test criteria of our own. The following sections describe the test setup and the test methods used, and list the products tested.

# Test environment

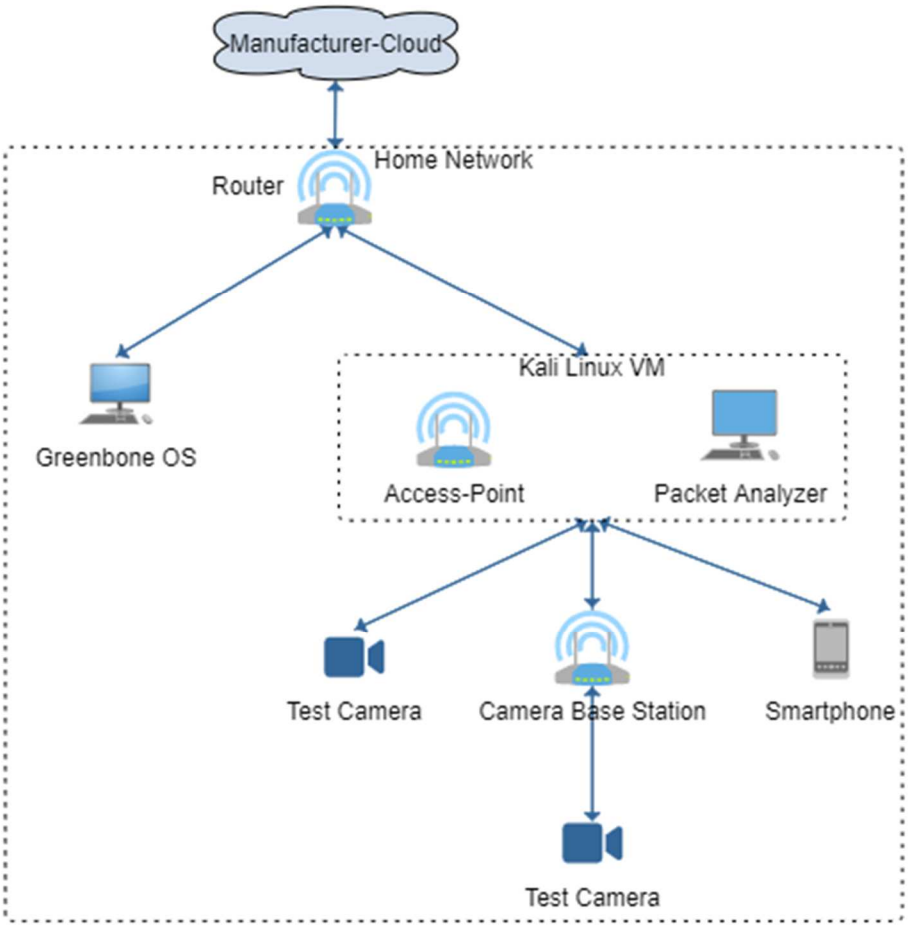


*Figure 1 – Test setup*

In a normal home network, the camera systems would connect to the home-network router, and from there to the manufacturer's cloud services. In the test, an additional network, controlled by a virtual Kali Linux[1] machine, was connected between the cameras and the home router. This structure allowed both the data traffic between cameras and cloud, and communications of the respective camera app with cameras and cloud, to be monitored.

In addition, a virtual machine with Greenbone OS and the OpenVAS Vulnerability Scanner[2] was used to check the cameras and base stations for open ports and vulnerabilities.

[1] https://www.kali.org
[2] https://www.openvas.org

# Test methods

## General security features

In this section of the test, the features offered by the camera systems were checked for their security properties. Security-relevant features include passwords, administration, firmware, as well as sharing recordings and access rights with other users. Information on the products' features was taken from the respective apps and product documentation.

## Network and packet analysis

To check the sending behaviour of the camera systems, the data traffic was redirected via a virtual machine with Kali Linux. This allowed the data sent by the camera systems to be recorded using the Wireshark[3] analysis tool.

The first step was to check whether the devices or the smartphone app send unencrypted data within the local network or to the manufacturer's servers.

In the next step, the mitmproxy[4] tool was used to simulate a man-in-the-middle attack on secure connections between the smartphone app and the manufacturer's servers. A self-created security certificate was installed on the smartphone.

The manipulated certificate was first installed as a user certificate. This step can be carried out by any smartphone user without root rights. If an application correctly checks security certificates, such an attempt at manipulation should be easy to recognize.

The certificate was then installed in the smartphone's system certificate-store using root access. Simple certificate checks cannot detect an untrusted certificate in this store, since the Android system itself regards certificates in the system store as trusted. Through techniques such as certificate pinning[5], however, it is still possible for apps to recognize an untrusted certificate.

Finally, using the network scanner nmap[6] and the OpenVAS Vulnerability Scanner, the camera systems were examined for possible weak points that could be exploited by attackers in the local network.

[3] https://www.wireshark.org
[4] https://mitmproxy.org
[5] https://developer.android.com/training/articles/security-config#CertificatePinning
[6] https://nmap.org

# Tested products

The following camera systems were checked as part of this test. For all products, the latest firmware and app versions available at the time of testing were used.

| Vendor | Product | Firmware | App Version |
|---|---|---|---|
| **Anker** | Eufycam 2C | 2.0.9.8h (Base station)<br>1.6.1 (Camera) | 1.7.4_581 |
| **Arlo** | Pro 3 | 1.16.1.3_495_1a608c1 (Base station)<br>1.060.10.18_749_4b65ff8 (Camera) | 2.16.2_28010 |
| **Blink** | XT2 | 2.13.18 (Sync Module)<br>7.96 (Camera) | 6.0.10_524400 |
| **Kami** | Dome X | 4.3.0.0C_201909250959 | 2.1.3_20200417 |
| **Nest** | Cam IQ Indoor | 4720014 | 5.50.0.7 |
| **Ring** | Stick Up Cam | 22.05.2020 (Version number not shown) | 3.26.0 |

# Test Results

In order to provide a better overview of the test results, the information collected is first summarized in a table, and then discussed in more detail in text form.

## Symbols

The following symbols were used to evaluate the test criteria:

| Symbol | Meaning |
|---|---|
| ● | "Yes", feature available |
| ◪ | "Partly", feature available but with limitations |
| ○ | "No", feature not available |
| n/a | "Not applicable", could not be tested. Please see detailed results |

| | Anker Eufycam 2C | Arlo Pro 3 | Blink XT2 | Kami Dome X | Nest Cam IQ | Ring Stick Up Camera |
|---|---|---|---|---|---|---|
| **Login/Password** | | | | | | |
| Check of password strength | ? | ● | ● | ● | ● | ? |
| Password requirements | 8-20 Characters | 8 Characters<br>Uppercase/lowercase<br>Number<br>Special characters | 8 Characters<br>Uppercase/lowercase<br>Number<br>Special characters | 8-16 Characters<br>Uppercase/lowercase<br>Number | 8 Characters<br>Letters<br>Number<br>Special characters | 8 Characters |
| Two-factor authentication (2FA) | ○ | ● | ○ | ○ | ● | ● |
| Lockout after failed login attempts | ● | ● | ● | ○ | ?[7] | ○ |
| **Wi-Fi connection** | | | | | | |
| Warning if network is unsecured | n/a | n/a | ● | ● | ○ | ○ |
| **Firmware** | | | | | | |
| Update during setup | ● | ● | ● | ● | n/a | ● |
| Automatic updates | ● | ● | ● | ● | ● | ● |
| Manual update available | ● | ● | ● | ● | ○ | ● |
| Secure firmware download (HTTPS) | ○ | ● | ● | ○ | n/a | ● |
| **Video transmission** | | | | | | |
| Secure transmission from/to the cloud | ● | ● | ● | ? | ? | ● |
| **Storage** | | | | | | |
| Cloud | ● | ● | ● | ● | ● | ● |
| Duration of cloud storage time can be configured | ○ | ○ | ● | ○ | ○ | ○ |
| Local | ● | ● | ○ | ○ | ○ | ○ |
| Network attached storage (NAS) | ● | ○ | ○ | ○ | ○ | ○ |
| **App** | | | | | | |
| User account with manufacturer required | ● | ● | ● | ● | ● | ● |
| Required permissions are appropriate | ● | ● | ● | ● | ● | ● |
| Logout from app possible | ● | ● | ● | ● | ● | ● |
| SSL certificate check | ● | ● | ● | ○ | ● | ● |
| SSL certificate check (system) | ● | ● | ○ | ○ | ○ | ● |

[7] Login with Google account; Captcha after multiple failed login attempts

| | Anker Eufycam 2C | Arlo Pro 3 | Blink XT2 | Kami Dome X | Nest Cam IQ | Ring Stick Up Camera |
|---|---|---|---|---|---|---|
| **Shared access** | | | | | | |
| **Other users** | | | | | | |
| Administration | ● | ● | ○ | ○ | ● | [8] |
| Live stream | ● | ● | ○ | ● | ● | ● |
| Recordings | ● | ● | ● | ● | ● | ● |
| Admin/non-Admin access configurable | ● | ● | n/a | n/a | ○ | ○ |
| **Public access via browser** | | | | | | |
| Access to live stream configurable | ○ | ○ | ○ | ○ | ● | ○ |
| Password protection configurable | ○ | ○ | ○ | ○ | ● | ○ |
| **Additional security tests** | | | | | | |
| OpenVAS: no vulnerabilities | ● | ● | ● | ● | ● | ● |
| Open ports | 554 (RTSP)[9] | ○ | 53 (DNS) | ○ | ○ | ○ |

[8] Not all settings are available to other app users
[9] Only open when the corresponding option is applied in the app

## Detailed results

*Setup & Login*

When creating a new user account, the apps of the **Anker Eufycam 2** and the **Ring Stick Up Camera** allow the use of insecure passwords. With these apps, easy-to-guess passwords, such as "password" can be used, which offer little protection against unauthorized access to the user account.

With the **Ring Stick Up Camera** app, however, this weak point can be compensated for by setting up two-factor authentication (2FA) using a security code sent by SMS. Even if users do not activate 2FA, they have to enter a security code sent by email after each login, in order to be able to use the functions of the app. The apps of the **Arlo Pro** and the **Nest Cam IQ** also offer this additional security function - the latter indirectly using login via a Google account.

The apps of the **Kami Dome X** and the **Ring Stick Up Camera** do not lock the user account after too many failed login attempts, thus offering little protection against brute-force password guessing attacks.

New users can only log in to the **Nest Cam IQ** using their Google account. If too many failed login attempts are made, a captcha code is required.
The apps of the remaining cameras lock the user account for a certain time after a few failed login attempts. This method, like the Captcha method, makes password guessing using a brute-force attack impractical.

When setting up the cameras for the first time, the **Ring Stick Up Camera** and the **Nest Cam IQ** can be connected to an unsecured wireless network without a warning being shown. Due to the relatively long range of Wi-Fi networks, the user's neighbours could also read data that is sent unencrypted in the local network.

The **Anker Eufycam 2C** and **Arlo Pro 3** camera systems use base stations that are connected to the router of the home network via a cable connection. Hence the "warning when connecting to an unsecured network" point is not relevant to these devices. The respective base stations of these two systems, like that of the **Blink XT2**, set up their own wireless networks to which the cameras connect. The networks created in this way are secured against unauthorized access with WPA2.

*Firmware*

With the exception of the **Nest Cam IQ**, all camera systems carry out an update of the device firmware (which is visible to the user) after the initial setup. According to the product documentation, all systems keep their respective firmware up to date via automatic updates. This prevents users from using firmware with potential security flaws after an update has been released.

The respective firmware installers of the **Kami Dome X** and the **Anker Eufycam 2C** are downloaded unencrypted via an HTTP connection, which poses a potential security risk due to manipulated firmware.

| Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 192.168.0.46 | 47.254.187.24 | HTTP | 284 | GET /yifirmware/smarthomecam/familymonitor-y32-manual/4.3.0.0C_201909250959restore.zip |
| 47.254.187.24 | 192.168.0.46 | TCP | 60 | 80 → 47528 [ACK] Seq=1 Ack=231 Win=30720 Len=0 |

*Figure 2 -- Kami Dome X: unencrypted firmware download*

| Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 192.168.0.88 | 52.219.72.132 | HTTP | 213 | GET /security/8312d3e2-2388-4a92-91b4-09448235ea47_eufy_2.0.9.8h_20200509.img |
| 52.219.72.132 | 192.168.0.88 | HTTP | 1095 | HTTP/1.1 200 OK |

*Figure 3 -- Anker Eufycam 2C: unencrypted firmware download*

*Video transmisson*

All camera systems send video recordings to their cloud servers exclusively in encrypted form.

**Kami Dome X** sends recordings over the HTTP protocol and uses proprietary encryption for the data sent. Although this procedure does not necessarily represent a security problem, it is more like a "security through obscurity" approach. The use of established encrypted transmission methods such as HTTPS / TLS would be preferable here. The live transmission of the video stream to the smartphone app takes place via a similarly proprietary-encrypted UDP connection.

| Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 10.42.0.69 | 47.254.187.8 | HTTP | 630 | POST / |
| 47.254.187.8 | 10.42.0.69 | HTTP | 360 | HTTP/1.1 200 OK |
| 47.254.187.8 | 10.42.0.69 | HTTP | 79 | HTTP/1.1 100 Continu |
| 47.254.187.8 | 10.42.0.69 | HTTP | 79 | HTTP/1.1 100 Continu |

*Figure 4 -- Kami Dome X: recordings transmitted via HTTP*

**Nest Cam IQ** uses the outdated version 1.0 of the TLS encryption protocol for the transmission of videos from the camera to the cloud, which is assessed as unsafe by popular web browsers. An upgrade to a newer version (1.2 / 1.3) is recommended here. When transferring from the cloud to the camera app, however, the newer protocol versions are used for the video download.

| Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 10.42.0.65 | 35.195.33.221 | TLSv1 | 153 | Client Hello |
| 35.195.33.221 | 10.42.0.65 | TCP | 66 | 443 → 47338 [ |
| 35.195.33.221 | 10.42.0.65 | TCP | 1474 | 443 → 47338 [ |
| 35.195.33.221 | 10.42.0.65 | TLSv1 | 265 | Server Hello, |

*Figure 5 – Nest Cam IQ: connection between camera and cloud via TLS 1.0*

*Storage*

Local storage of video recordings allows users full control over the recorded data without having to rely on the manufacturer to handle the data securely. Only two of the camera systems tested allow recorded videos to be saved locally.

A USB storage device can be connected to the base station of the **Arlo Pro 3** to save video recordings on it instead of in the cloud.

16GB of storage is already integrated in the base station of the **Anker Eufycam 2C**, which can be used for storing recordings. In addition, recordings can also be sent via RTSP to a network storage device (NAS) in the user's local network. Only event recordings are transmitted, e.g. triggered by motion detection. Although the RTSP protocol supports securing the transmitted stream using passwords, no password can be set in the app. This means that every user in the local network can read the transmitted recordings.

*App*

All apps of the tested cameras only request those permissions on the smartphone that are necessary for the functioning of the app.

For some apps, however, it would be desirable if they gave the user further information as to why the particular permissions had been requested. For example, the apps of **Kami Dome X** and **Anker Eufycam 2C** ask for permission to use the phone's location function when attaching the cameras. However, it is not clear from the setup process why this authorization is required.

The **Ring Stick Up Camera** app does not provide a more precise explanation of the requested location authorization either. However, at least it informs the user that the authorization is only required during setup and can be withdrawn afterwards.

In order to successfully carry out a man-in-the-middle attack on secure TLS connections, it is usually necessary to "convince" the client (in our case the smartphone with the manufacturer app) that a security certificate created by the attacker is trustworthy. However, this step is not necessary to decrypt the data sent by the **Kami Dome X** app - the app seems to skip the verification of the TLS certificates, and accepts any certificate without warning.


```
"isNew": true,
"message": "",
"model": "17",
"name": "Kami Camera",
"nickname": "YI_[redacted]",
"online": true,
"password": "[redacted]",
"share": false,
"state": 1,
"type": 2,
"uid": "[redacted]"
```


*Figure 6 -- Kami Dome X: account and camera information*

Figure 6 shows a section of a data packet that could be read by a man-in-the-middle attack. Among other things, the account name, the identification number of the connected camera and a password hash are transmitted. Due to the use of proprietary encryption, the transmitted video data could not be decrypted using this approach. Nevertheless, the lack of certificate verification poses a security risk.

Even with a certificate marked as trustworthy, the apps of the **Anker Eufycam 2C**, **Ring Stick Up Camera** and **Arlo Pro 3** denied access to the user account and the cameras, so that in the test no man-in-the-middle attack on transmitted app data was possible.

The **Nest Cam IQ** app and the **Blink XT2** perform a proper security certificate check, but trust the system storage certificates. A more detailed examination of the certificates would be recommended here.

*Shared access*

The apps from all manufacturers allow other users at least limited access to camera data.

All cameras but the **Kami Dome X** and the **Blink XT2** allow the creation of administrator users. In addition to accessing camera recordings, administrator users may also change the configurations of the connected cameras, such as video and audio settings.

The apps of the **Anker Eufycam 2C** and **Arlo Pro 3** allow the creation of both administrator- and restricted users. While restricted users only have access to the video recordings, administrator users have full access to all features.

In the **Nest Cam IQ** app, users can publish the live stream from the camera. The stream can then also be opened in a browser via a link, without needing the app. Access to this stream can also be protected with a password.

*Further security tests*

None of the cameras or base stations use services which, according to the results of the OpenVAS scanner, have vulnerabilities that can be attacked. By default, no critical ports are open in the local network.

# Summary

A security deficiency was found in the **Anker Eufycam 2C**. The unencrypted download of firmware updates could allow manipulation of the device firmware. The smartphone app accepts weak passwords for the user account, but after a few unsuccessful login attempts, an account lock prevents further attempts at guessing the password. Due to the possibility of local recording, users can also use the camera without sending their recordings to the manufacturer's cloud server. In the case of local storage, the internal memory of the base station is preferred, since data transmitted to local network storage is not encrypted.

With the **Arlo Pro 3** camera system, no security deficiencies were found in the test. Users can also save video recordings locally without sending them to the manufacturer's cloud server.

The **Blink XT2** camera system was largely positive in the test. However, the verification of security certificates by the smartphone app could be improved. Otherwise, no further security deficiencies were found.

A number of security deficiencies were found in the test of **Kami Dome X**: the device firmware is downloaded unencrypted using the camera app. When transmitting video recordings to the manufacturer's cloud servers, the camera uses its own encryption methods instead of using proven transmission methods such as HTTPS / TLS. Since the camera app does not check the security certificates, a man-in-the-middle attack is possible even without installing a manipulated certificate on the victim's smartphone.

The **Nest Cam IQ** was largely positive in the test. One drawback is the use of the outdated TLS version 1.0 protocol for the transmission of video data from the camera to the manufacturer cloud. The verification of security certificates by the smartphone app could be improved.

The **Ring Stick Up Camera** largely performed well in the test. The only points of criticism are the permission to assign weak passwords for user accounts and the lack of a lockout mechanism in the event of too many failed login attempts. Otherwise, no security deficiencies were found.

# Copyright and Disclaimer

This publication is Copyright © 2020 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(June 2020)