Wired Camera IoXT Assessment

Google

September 21, 2021 – Version 2.0

Prepared for

Angelina Sosa
Ankur Chakraborty

Prepared by

NCC Group ioXt Test Lab

Executive Summary

Overview and Scope

NCC Group was contracted by Google to conduct a security assessment of the Nest Cam (wired) device. This assessment was specifically focused on determining whether the device complies with The ioXt Security Pledge.[1] This assessment was performed during August, and was authorized by Google.

The device being assessed is a wire powered wifi residential network camera. A "development" and production device were provided. The firmware version for the devices was:

- 1.57 OPENMASTER 267754 stable-channel

Key Findings

Within the black-box test methodology, the security posture of the production device was found to be strong. All wireless traffic was secured using best practices, with up to date TLS. Factory reset functionality reset the device to its original state securely. Google provided information regarding security of firmware integrity and update protections, as well as encryption of data at rest. An unprivileged production-testing debug service was available via TCP which was demonstrated to be unavailable in the production build.

With respect to the ioXt Residential Camera Profile, both devices met the minimum certification requirements, but some of the maximum level requirements were not met: sensitive cloud data is not encrypted on a per user basis at the current time. Documentary evidence of hardware-based power side channel protections were provided.

Limitations

All assessments performed as part of the ioXt pledge certification program are intended to be time-limited black box audits. These reviews are simply focused on determining the basic security hygiene of the product and the compliance with the eight pledge principles. Therefore, NCC Group performed this shallow review in a limited time-frame, and did not explore deeply any portion of the device. In particular, NCC Group did not review the kernel, or look for remotely-exploitable memory corruption issues in network-listening services. A white box based assessment is anticipated to go into further depth.

[1] https://www.ioxtalliance.org/the-pledge

Compliance Summary

This section serves to summarize the device's compliance with the ioXt Residential Camera Profile version 1.0[2]

Principle	Level	Justification
Automatically applied updates	2/2	Software updates are supported, with a software maintenance and update process in use. These updates are made available to impacted users. Together these meet the requirements for Automatic Updates level 1. These updates are applied automatically when product usage allows and update process which occurs at non-predictable intervals which will be unpredictable across a fleet.
Vulnerability reporting program	4/4	Client described the vulnerability reporting program applicable to this and many other devices.[3] NCC Group has confirmed that this program meets the ioXt requirements, including ISO29147[4] compliance. Additionally, this program accepts external researcher submissions, and meets acceptance criteria for monitoring security relevant components. A public researcher rewards program was in place.
Security expiration date	1/1	Google will publish security EOL data for this device at https://support.google.com/product-documentation/answer/10231940, with security expiration date set at device release date plus 5 years.
No universal passwords	3/3	While the device itself does not require authentication for a user to interact with it physically, Google Home account credentials are required to remotely interact with the device, and these credentials, along with WLAN connectivity, are required to render the device operable. Note also that Client account authentication can be backed by two-factor authentication, and once 2fa requirements are enabled these are enforced on the remote account.
Proven cryptography	2/2	Google provided a broad description of the cryptography used in various aspects of device functionality including network communication, firmware verification, and provisioning. The cryptography choices were reviewed and compliant with currently accepted best practices.
Secure by default	2/2	The device returns to its initialization state after factory reset and is no longer able to access the WiFi network it was connected to. The device also had no externally accessible storage available.

[2] https://www.ioxtalliance.org/s/ioXt_Residential_Camera_Profile.pdf
[3] https://www.google.com/about/appsecurity/reward-program/
[4] https://www.iso.org/standard/72311.html

Principle	Level	Justification
Secured interfaces	2/4	A remote port scan was performed. Openweave was enabled on port 11095. All sensitive traffic was protected by TLS 1.2 and TLS 1.3. BLE communication made use of well-known cryptography methods and protocols. An AMLogic USB device is enumerable via the external USB port when the device is sufficiently powered. No public USB drivers exist for its particular vendor/product ID pair, but it is understood that this is intended to be used for privileged engineers to reflash the device. No method was identified to interact unauthenticated with this interface during assessment. Google engineers confirmed that this port is only able to perform encrypted and authenticated updates. Sensitive cloud data is not encrypted on a per-account basis (SI117) (required for level 3). Documentation of hardware based side channel protections were available for the main processor chip in use preventing power side channel analysis.
Verified software	4/4	Google has a maintenance plan that provides regular patches for high severity updates. Software file systems are integrity checked, with *noexec* on mutable partitions. A secure boot mechanism based on hardware root of trust is in place with anti-rollback protection based on eFuses.

ioXt Security Pledge Methodology

This section describes the criteria used by NCC Group when testing a product for alignment with the ioXt Security Pledge. While many of the questions posed below are answered manually by reviewing and testing the product, in the interest of time, some may be answered based on the *ioXt Pledge Questionnaire* that the OEM fills out to provide NCC Group with a detailed technical understanding of the product and its security controls.

The set of tests that were explicitly performed are detailed in the member-accessible ioXt Test Case Library. This summary provides a broader perspective of the considerations that NCC Group reviewed in alignment with the overall ioXt pledge.

The ioXt Security Pledge is composed of eight clear principles:

1 No universal passwords

The pledge states:

> *The product shall not have a universal password; unique security credentials will be required for operation.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the device:

- All device passwords are unique at the earliest opportunity (out-of-box experience or manufacturing) and not resettable to any universal default value.
- The minimum strength and verification method of the password render brute force attacks difficult even at scale.
- The device does not use any hard-coded credentials or identity.

With respect to any methods by which the device authenticates to remote endpoints and functionality, NCC Group further reviewed the following:

- Establish the set of identifiers that uniquely identify a device and consider the use and sensitivity of each.
- Establish that each device must prove its unique identity and authenticate to exercise any remote functionality using a proven secure mechanism.

2 Secured interfaces

The pledge states:

> *All product interfaces shall be appropriately secured by the manufacturer.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the device:

- JTAG/SWD and debug interfaces are disabled on release products.
- All sensitive interfaces, including device-internal interfaces, are encrypted and authenticated.
- Authorization is performed for any privileged access to device functionality.
- Sufficient input validation is performed on all external interfaces.

3 Proven cryptography

The pledge states:

> *Product security shall use strong, proven, updatable cryptography using open, peer-reviewed methods and algorithms.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the device:

- Establish where the product uses cryptography.
- Establish that wherever cryptography is used, it is considered standard and best-practice.
- Establish that wherever TLS is used, it is version 1.2 or greater.

4 Security by default

The pledge states:

> *Product security shall be appropriately enabled by default by the manufacturer.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the device:

- There are no RMA/debug modes enabled in release firmware.
- There are appropriately implemented privacy modes/buttons.
- There is no means to trivially bypass user authentication.
- All device keys are managed securely.
- There are no unnecessary network-facing services, and those that are necessary restrict access accordingly.
- The manufacturer provides consumers with clear and transparent information about how their personal data is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.
- Where personal data is processed on the basis of consumers' consent, this consent is obtained in a valid way, and that consent is revocable by the consumers at any time, allowing the consumers to permanently delete all previously collected data and prevent future collection.
- Logging on the device does not expose personal private information of the user.

5 Signed software updates

The pledge states:

> *The product shall only support signed software updates.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the device:

- Firmware updates are downloaded over TLS, and the certificate of the firmware host that the device verifies should be pinned.
- The firmware images are encrypted until installation.
- The firmware images are signed, and they are verified on the device prior to installation.
- The device supports secure boot.
- The device supports downgrade prevention.

6 Automatically applied updates

The pledge states:

> *The manufacturer shall act quickly to apply timely security updates.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the manufacturer:

- The device supports a secure firmware over-the-air update mechanism.
- The manufacturer is able to distribute firmware updates remotely using this mechanism.
- The consumer can be informed in a timely manner that an update is required or available. The urgency of each update is communicated to the consumer.
- Where possible, the device will continue to provide a basic level of functionality during an update.
- The manufacturer maintains awareness of both internally developed and externally sourced firmware running on the device and is responsive in distributing updates to both in the presence of a discovered vulnerability.

7 Vulnerability reporting program

The pledge states:

> *The manufacturer shall implement a vulnerability reporting program, which will be addressed in a timely manner.*

In order to test this best-practice, NCC Group engaged the manufacturer to answer the following questions:

- Have you ever had to deal with an external security vulnerability report?

- Have you defined patching criteria which guarantee that vulnerabilities must be patched within a reasonable time frame from initial disclosure?
- When a security update is published, how are vulnerability details disclosed publicly to stakeholders including customers?

Furthermore, NCC Group has reviewed the following aspects of the manufacturer:

- Security contact information and vulnerability reporting guidelines are published on the manufacturer's website.
- The contact information is easily discoverable.
- Any documentation provided by the company related to the their vulnerability disclosure program and its parameters.
- The company participates in a bug bounty program, and the details thereof.

8 Security expiration date

The pledge states:

> *The manufacturer shall be transparent about the period of time that security updates will be provided.*

In order to test this best-practice, NCC Group engaged the manufacturer to answer the following questions:

- After the product is released, what is the earliest possible date that it will no longer be supported via security patches before *End Of Life*?
- How is this information communicated to stakeholders including customers?