Nest Wifi Router and AP ioXt Assessment

Google

August 11, 2021 – Version 2.0

Prepared for

Ankur Chakraborty
Medha Jain

Prepared by

NCC Group ioXt Validation Lab

Executive Summary

Overview and Scope

NCC Group was contracted by Google to conduct a security assessment of the Nest Wifi router and AP devices. This assessment was specifically focused on determining whether the pair of devices comply with The ioXt Security Pledge.[1] This assessment was performed in January 2021, with some follow-up testing in June 2021, and was authorized by Google.

The devices being assessed are a Wifi router device and a smart speaker device with Wifi Access Point functionality, sold as a pair. Two sets of "production" devices were purchased from the Google public storefront for the test. The firmware versions for the devices is:

Nest Wifi router:

```
Software version: 13099.118.19
```

Nest Wifi AP:

```
Firmware version: 229149
Cast software version: 1.50.229149
```

Key Findings

Within the test parameters, the security posture of the production devices was found to be strong. After re-testing, physical interfaces were restricted or unavailable on production devices, all BLE and WLAN communication was secured using best-practices, namely up-to-date TLS, except for services specifically for compatibility with legacy devices. Testing additionally found factory reset functionality removed user private data, and Google provided documentation regarding the security pertaining to firmware integrity assurances and the data storage protections used by the devices.

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 deeply explore any portion of the devices. For instance, NCC Group did not review the kernel, or look for remotely-exploitable memory corruption issues in network-listening services. This type of work is best suited for a white-box audit where product source code is available.

Additionally, a number of relevant services and applications were out of scope for the purposes of this assessment. In particular, NCC Group did not assess the back-end microservices or perform an assessment of the applications running on the devices. The companion mobile application was also out of scope.

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

Nest Wifi Router and AP Pledge Compliance Summary

This section serves to summarize the devices' compliance with the ioXt Base Profile 1.0[2] which have been defined by the ioXt Alliance. The Nest Wifi AP device in particular also contains smart speaker capabilities, however no information regarding this was provided by Google to be able to test the compliance with the ioXt Smart Speaker profile.[3]

Principle	Level	Justification
Automatically Applied Updates	2/2	An update was performed automatically when the devices were first connected to the Internet, without requiring any user interaction. Google indicated that the devices receive regular updates, including security fixes, and that updates are always applied automatically.
Security Expiration Date	1/1	Google shared internal documentation regarding the EOL support of various devices including these, meeting the requirements of this pledge item. Google indicated that this information will be publicly available at by July 30, 2021.
Vulnerability Reporting Program	4/4	Nest products are included within the Vulnerability Reporting Program.[4] This program is open to external submissions, and, as all updates are applied automatically, there are no parties that must take action, and therefore no need for notifications. Also, the VRP contains a Researcher Rewards Program indicating requirements, terms and rewards for the submission of security issues.
Verified Software	3/3	Google has a maintenance plan that regularly provides patches including security updates. Software is signed and verified before it runs on the devices and the Trusted Platform Module maintains the current OTA version, with an anti-rollback mechanism protecting from loading older, compromised images.
No Universal Passwords	2/2	NCC Group was not able to find any universal passwords used on this product. Google confirmed that there are no universal or hard-coded secrets.
Proven Cryptography	2/2	Google provided a broad description of the cryptography used in various aspects of device functionality including data-at-rest storage, network communication, firmware verification, and provisioning. The cryptography choices were reviewed and found compliant with currently accepted best practices. However, several services still accepted TLS 1.0 connections, which is considered deprecated and is affected by several vulnerabilities.
Secured Interfaces	3/3	With the exception of the encrypted firmware OTA, and requests to generate 204 responses, all observed remote traffic was secured by TLS 1.2 and TLS 1.3. A remote port scan found no directly exposed ports. This satisfies the only secured interface requirement in the Base Profile (SI1). The proximity attack portion of secured interfaces (SI2) was also met. Google documented two open TCP ports on the WLAN providing services for compatibility with legacy devices that allow unencrypted HTTP traffic or accept TLS 1.0. However, these services did not contain any sensitive information, and also supported newer TLS versions and had downgrade attack prevention, mitigating any potential attack for these services. No local interfaces were found to expose insecure services meeting secured interfaces local attack (SI3).

[2] https://www.ioxtalliance.org/s/ioXt_2020_Base_Profile_1_1.pdf
[3] https://www.ioxtalliance.org/s/ioXt_Smart_Speaker_Profile-V1_0.pdf
[4] https://www.google.com/about/appsecurity/reward-program/index.html

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 reset-table 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?