Nest Thermostat ioXt Device Assessment

Google

June 4, 2021 – Version 1.0

Prepared for

Ankur Chakraborty
Medha Jain

Prepared by

NCC Group ioXt Certification Lab

Executive Summary

Overview and Scope

NCC Group was contracted by Google to conduct a security assessment of the Nest Thermostat device. This assessment was specifically focused on determining whether the device complies with The ioXt Security Pledge.[1] This assessment was performed in over a period in September and October of 2020, and was authorized by Google.

The device being assessed allows a user to exercise its functionality via the capacitive sensor user interface, the accompanying smartphone application, and other connected Google home devices. The mobile companion application and a smart speaker device were used for testing, but were not considered to be in scope of this test. Google provided two devices for test, referred in this document as the "production" and "development" devices respectively. The hardware model numbers, firmware versions, and serial numbers for the devices are:

Production Device:

```
"Bootloader 1.0d1-dvt-10"
"Software: FSI Retail"
"HW version = DVT_1"
"Z1:932b8b79d7692a01"
```

Development Device:

```
"Bootloader 1.0d1-dvt-14-V"
"Software: FSI Dev"
"HW version = DVT_1"
"Z1:932b8b79d7213e28"
```

Key Findings

Within the test parameters, the security posture of the production device was found to be strong. Interfaces exposed on the development device were restricted or unavailable on production, all BLE and WLAN communication was secured using best-practices, namely up-to-date TLS and Weave,[2] 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 device.

With respect to the ioXt base profile, the device met all requirements with the exception of providing public information regarding the duration of product support, which Google has indicated will be available at a time before product release. NCC Group will verify this when it is available.

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. 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 Android applications running on the device. The companion mobile application was also out of scope.

[1] https://www.ioxtalliance.org/the-pledge
[2] https://openweave.io/documents/openweave-security.pdf

ioXt Pledge Compliance Summary

This section serves to summarize the device's compliance with the ioXt Base Profile[3] which have been defined by the ioXt Alliance.

Principle	Level	Justification
Automatically Applied Updates.	2/2	While no update was performed, Google provided extensive documentation on how remote updates are implemented. Google indicated that although updates are applied automatically, users are made aware of an update via the device Settings menu.
Security Expiration Date	1/1	Google shared internal documentation regarding the EOL support of various devices including this one, meeting the requirements of this pledge item. Google indicated that this information will be publicly available at https://support.google.com/product-documentation/answer/10231940 by July 30, 2021.
Vulnerability Reporting Program	4/4	Google indicated this product is included in the reporting program.[4] The VRP is open to external submissions and is committed to timely responses (both an automated response and case number), provides an expected triage time and response time of 5 days.
Verified Software	4/4	Google has an maintenance plan that provides quarterly patches of high severity updates. Software is signed and verified (starting with the bootloader being verified by NXP's High Assurance Boot (HAB)[5] implementation) before it runs on the device and an anti-rollback mechanism protects from loading older, compromised images.
No Universal Passwords	1/1	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 compliant with currently accepted best practices.
Secured Interfaces	3/3	With the exception of one empty HTTP GET during device pairing, all traffic observed was secured by TLS 1.2 and TLS 1.3. A remote port scan was performed. No ports were directly exposed remotely by design of the device. On the WLAN, while outside of the scope of the base profile, the device made available two services listening on TCP ports, both secured.

[3] ioXt Base Profile
[4] https://www.google.com/about/appsecurity/reward-program/index.html
[5] https://www.nxp.com/docs/en/application-note/AN12263.pdf

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 ioXt Test Case Library.[6] 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:

[6] https://ioxtalliancemembers.org/wg/Compliance_wg/document/134

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. The manufacturer
- 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?