Nest Hub Max ioXt Assessment

Google

June 4, 2021 – Version 1.0

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 Hub Max 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 January 2021, with some follow-up testing in May 2021, and was authorized by Google.

The device being assessed is a smart speaker device with a display. Two "production" devices were purchased from the Google public storefront for the test. The firmware version for the devices is:

```
Software version: 36.13.18.363046951
Chromecast firmware version: 1.54.250320
```

Key Findings

Within the test parameters, the security posture of the production device 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, 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 Smart Speaker Profile, the device met the minimum certification requirements, but some of the higher level requirements were not met, as further described in the following section.

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

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

Nest Hub Max Pledge Compliance Summary

This section serves to summarize the devices' compliance with the ioXt Smart Speaker Profile[2] version 2.00, which has been defined by the ioXt Alliance.

Principle	Level	Justification
Automatically applied updates	2/2	An update was performed automatically when the devices were first set up. Users are made aware of an update from screen output messages. Additionally, client provided extensive documentation on how remote updates are implemented.
Vulnerability reporting program	4/4	Client indicated these products are included in the vulnerability reward program.[3] The VRP is open to external submissions and is committed to timely responses (both an automated response and case number).
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.
No universal passwords	2/2	NCC Group was not able to find any universal passwords used on this product. The test indicates that a device that does not implement 2FA automatically meets this test's acceptance criteria, requiring only that 2FA is enforced if implemented. The devices do not implement user authentication for voice operation, and requires both the user's Google account credentials and WiFi credentials to operate over a network interface.
Proven cryptography	2/2	Google provided a broad description of the cryptography used in various aspects of devices functionality including network communication, firmware verification, and provisioning. The cryptography choices were reviewed and compliant with currently accepted best practices. It should be noted that the devices allowed the deprecated TLS 1.0 protocol for communication, captured in *Secured Interfaces*
Security by default	2/2	The devices return to their initialization state after a factory reset and are no longer associated to the user account and the network to which it was previously connected. Personalized commands that require access to a user's personal information can be gated by voice recognition. NCC Group confirmed that an unknown voice could not exercise this behavior when voice recognition was enabled.

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

Principle	Level	Justification
Secured interfaces	2/4	Device traffic was protected by TLS 1.2 and TLS 1.3 in most cases. Similarly, the BLE and WiFi interfaces seemed to be properly secured. A remote port scan was performed. No ports were directly exposed remotely by design of the devices and all ports exposed (such as 8008, 8009, 8443, etc.) on the WiFi interface were indicated within documentation. Security levels 3 and 4 were determined to not be met. The microphone is not optically shielded (SI102), and therefore theoretically vulnerable to lightcommands attacks. Information about encryption of data stored into the flash filesystem was not provided (SI104). Furthermore, no specific documentation could be found regarding the main SoC's broad protection measures against power side-channel attacks (SI106), a requirement necessary for security level 4. It is important to note however that the devices meet most of the test cases required to meet security levels 3 and 4. Aside from those described above, physical interfaces were determined to be disabled (SI3.1), although no information was provided for debug ports. The microphone mute switch and LED indicator are implemented in hardware, protecting them from influence by misbehaving or compromised software (SI108).
Verified software	4/4	Google has a maintenance plan that regularly provides patches of high severity updates. Software is signed and verified before it runs on the devices and an anti-rollback mechanism protects from loading older, compromised images. Information on Secure Boot based on hardware root of trust (VS6) pertaining to the AmLogic SoC was provided, including eFuse-based rollback protection (VS7).

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?