Pixel 4/4XL and Pixel 4a ioXt Audit

Google

August 13, 2020 – Version 2.0

Prepared for
Eugene Liderman
Billy Lau
Sam Schumacher
Xevi Miro Bruix

Prepared by
NCC Group ioXt Certification Lab

Overview and Scope

NCC Group was contracted by Google to conduct a security assessment of the Pixel 4, Pixel 4XL, and Pixel 4a devices. This assessment was specifically focused on determining whether the devices comply with the ioXt Android Profile based on the ioXt Security Pledge.[1] This assessment was performed between July 28 and August 7, 2020, and was authorized by Google.

The overall assessment methodology is described in detail in ioXt Security Pledge Methodology on the following page, and included a technical review comparing the product design with the pledge requirements.

The hardware model numbers and firmware versions within the scope of this test are listed below:

- Pixel 4
  - Model: G020I/M/N
  - Version: QD4A.200805.001
- Pixel 4 XL
  - Model: G020P/Q/J
  - Version: QD4A.200805.001
- Pixel 4a
  - Model: G025J/M/N
  - Version: QD4A.200805.003 for USA, QD4A.200805.001 for RoW

Key Findings

The ioXt pledge compliance summaries for both the Pixel 4, Pixel 4 XL, and Pixel 4a device can be found in the following sections of this document.

Limitations

This assessment, performed as part of the ioXt certification program,[2] was a time-limited audit. These reviews are focused on determining the basic security hygiene of the product and the compliance with the eight pledge principles. Furthermore, the Android ioXt Profile relies heavily on public information about the device being tested, and leverages the GMS certification status of the product in order to demonstrate evidence for multiple ioXt pledge categories. The Pixel 4a device, being unreleased at the time of this assessment, was not officially GMS certified, and so did not satisfy some of these requirements. It was understood, however, that the Pixel 4a would be subject to the same requirements of previous devices including the Pixel 4, and that this device would be GMS certified prior to release. NCC Group made note of this in its submission to the ioXt Alliance. ***Update:*** *by the time this report was published, the Pixel 4a's GMS certification was also published, and that is now reflected in the table and references below.*

This assessment was focused exclusively on compliance with the ioXt certification program, and was not focused on identifying platform vulnerabilities beyond the scope of ioXt requirements.

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

[2] https://www.ioxtalliance.org/get-ioxt-certified

The ioXt Alliance is a group of technology industry leaders working to create practical standards to secure Internet of Things (IoT) devices. The ioXt Alliance security standards are based on the eight principles stated in the ioXt Security Pledge[3]:

1. The product shall not have a universal password; unique security credentials will be required for operation.
2. All product interfaces shall be appropriately secured by the manufacturer.
3. Product security shall use strong, proven, updatable cryptography using open, peer-reviewed methods and algorithms.
4. Product security shall be appropriately enabled by default by the manufacturer.
5. The product shall only support signed software updates.
6. The manufacturer shall act quickly to apply timely security updates.
7. The manufacturer shall implement a vulnerability reporting program, which will be addressed in a timely manner.
8. The manufacturer shall be transparent about the period of time that security updates will be provided.

The ioXt Alliance defines multiple profiles corresponding to various device classes, such as smart speakers and Android devices. The ioXt 2020 Base Profile[4] defines security requirements applicable to most or all IoT devices. Test cases verified for compliance with ioXt profiles are defined in the ioXt Alliance Compliance Test Case Library.[5] The requirements of the ioXt Android Profile 1.00[6] are effectively a superset of applicable requirements of the ioXt 2020 Base Profile. However, Base Profile test cases that duplicate requirements for Google Mobile Services (GMS) certification are omitted to simplify the certification process. Devices certified under the ioXt Android Profile 1.00 must qualify under the GMS certification process, or equivalent.

The Android Profile defines a set of security levels for each pledge item, 1 being the minimum requirement for certification, increasing with additional tests and requirements.

The Google Pixel 4, Pixel 4XL, and Pixel 4a devices were assessed against the ioXt Android Profile, version 1.00, using test cases defined in the ioXt Alliance Compliance Test Case Library, version 3.00.

Uraniborg Tool and Preloaded Applications Risk

The Android Device Security Database, a consortium consisting of researchers from the University of Cambridge and Johannes Kepler University Linz, created a risk scoring methodology to assess the cumulative risk of preloaded applications on Android devices. This scoring system computes the overall risk by quantifying and aggregating the risk associated with platform-signed applications, pre-granted permissions on preloaded applications, and application that communicate using cleartext traffic.

Google, in partnership with the university consortium, developed and released Uraniborg, an open source tool to automate the analysis of the attributes of preloaded applications on an Android device.

NCC Group has reviewed the both the method and the implementation of this tool, and used it to determine the preloaded application risk of these evaluated devices, which is the criteria for the requirements associated with *Security by Default* pledge item summarized in the subsequent sections.

[3] https://www.ioxtalliance.org/the-pledge
[4] https://ioxtalliancemembers.org/wg/Compliance_wg/document/135
[5] https://ioxtalliancemembers.org/wg/Compliance_wg/document/134
[6] https://ioxtalliancemembers.org/wg/Compliance_wg/document/153

This section serves to document the devices' compliance with the ioXt Android Profile,[7] which has been defined by the ioXt Alliance. The ioXt Alliance publishes device certifications on their website.[8]

Principle	Level	Justification
No universal passwords	4 / 4	The Pixel 4 device satisfies requirements that the device be GMS certified, and NCC Group reviewed a supplemental biometric compliance report establishing the strong biometric authentication mechanism subject to Android Compatibility Definition requirements.
Secured interfaces	3 / 3	The Pixel 4 device is GMS certified, satisfying the only requirement in this category.
Proven cryptography	3 / 3	The Pixel 4 device satisfies requirements that the device be GMS certified and that it is on the NIAP approved list.[9]
Signed software updates	6 / 6	The Pixel 4 device satisfies requirements that the device be GMS certified and that the average update time is less than 35 days.
Automatically applied updates	5 / 5	The Pixel 4 device meets requirements that the device be GMS certified, that the patch install rate is greater than 70%, and that updates are automatically deployed.
Vulnerability reporting program	4 / 4	The Pixel 4 is part of Google's reward program.[10] NCC Group reviewed and confirmed this program's compliance with ISO 29417:2018 (Section 9.2).[11] The program was further determined to comply with the other ioXt requirements that the program notify impacted parties, accepts external submissions, and covers security-relevant components within the Pixel 4 device.
Security expiration date	3 / 4	The Pixel 4 device satisfies requirements that an end of life policy is published, and that three years of support[12] are provided after launch. The highest level 4 was not satisfied because the device support window is shorter than four years.
Security by default	4 / 4	The Pixel 4 device is GMS certified. NCC Group reviewed the results of the Uraniborg tool (ioXt Security Pledge Methodology on the previous page) and established that the Pixel 4 preloads risk was was very low when considered against the set of over 50 Android devices measured by this tool.

[7] https://ioxtalliancemembers.org/wg/Compliance_wg/document/153
[8] https://compliance.ioxtalliance.org/products
[9] https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11019?
[10] https://www.google.com/about/appsecurity/android-rewards/
[11] https://www.iso.org/standard/72311.html
[12] https://support.google.com/pixelphone/answer/4457705?hl=en

Pixel 4a - ioXt Pledge Compliance Summary

This section serves to document the device's compliance with the ioXt Android Profile,[13] which has been defined by the ioXt Alliance. The ioXt Alliance publishes device certifications on their website.[14]

Principle	Level	Justification
No universal passwords	4 / 4	The Pixel 4a device satisfies requirements that the device be GMS certified, and NCC Group reviewed a supplemental biometric compliance report establishing the strong biometric authentication mechanism subject to Android Compatibility Definition requirements.
Secured interfaces	3 / 3	The Pixel 4a device is GMS certified, satisfying the only requirement in this category.
Proven cryptography	3 / 3	Google provided evidence that this device is in NIAP evaluation.
Signed software updates	6 / 6	Due to the fact that the Pixel 4a device has not been released, it is not possible to measure the average time between security updates. However, this category has been given a "met" rating due to Google's stated commitment to ensure that the Pixel 4a device will receive monthly security updates, and based on the precedent they have set with previous Pixel devices.
Automatically applied updates	5 / 5	The Pixel 4a device is not yet released, though Google intends to follow the same security update standards that are in place for the previous generations of Pixel phones. Because Google has demonstrated an install patch rate well above 70% for similar past devices including the Pixel 4 and Pixel 3a, this test criteria was accepted.
Vulnerability reporting program	4 / 4	The Pixel 4a is part of Google's reward program.[15] NCC Group reviewed and confirmed this program's compliance with ISO 29417:2018 (Section 9.2).[16] The program was further determined to comply with the other ioXt requirements that the program notify impacted parties, accepts external submissions, and covers security-relevant components within the Pixel 4a device.
Security expiration date	3 / 4	The Pixel 4a device satisfies requirements that an end of life policy is published, and that three years of support[17] are provided after launch. The highest level 4 was not satisfied because the device support window is shorter than four years.
Security by default	4 / 4	The Pixel 4a device is GMS certified. NCC Group reviewed the results of the Uraniborg tool (ioXt Security Pledge Methodology on page 3) and established that the Pixel 4a preloads risk was very low when considered against the set of over 50 Android devices measured by this tool.

[13] https://ioxtalliancemembers.org/wg/Compliance_wg/document/153
[14] https://compliance.ioxtalliance.org/products
[15] https://www.google.com/about/appsecurity/android-rewards/
[16] https://www.iso.org/standard/72311.html
[17] https://support.google.com/pixelphone/answer/4457705?hl=en