ETSI EN 303 645
Google Nest Wifi Pro
2022

Prepared by

DEKRA
Cybersecurity Hub

Executive Summary

Overview and Scope

DEKRA was contracted by Google to conduct a security assessment of the Google Nest Wifi Pro device. This assessment was specifically focused on determining whether the device complies with ETSI EN 303 645 Cyber Security for Consumer IoT: Baseline Requirements v2.1.1 using ETSI TS 103 701 Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements v1.1.1. This assessment was performed during September and was authorized by Google.

The device being assessed is a Wi-Fi router that allows users to create independent wireless connections for guests using different passwords. A "development" and production device were provided. The firmware and model version for the devices was:

- Model: G6ZUC
- FW: 1.63.324946

Key Findings

Device is in compliance with ETSI EN 303 645 v2.1.1 all the mandatory provisions and most of recommended ones following the procedures defined in ETSI TS 103 701 v1.1.1.

Within the compliance criteria, the security posture of the production device was found to be strong. No default passwords were used, vulnerability disclosure mechanisms were identified, software updates are properly secured, sensitive security parameters were protected using TEE, all BLE and WLAN communication was secured using best-practices, namely up-to-date TLS, Physical interfaces were restricted or unavailable on production devices, attack surface were reduced to the minimum services required and system was resilient to outages and all data protection provisions were met.

Google Nest Wifi Pro Compliance Summary

This section serves to summarize the accredited test report of **ISO 17025**.

Item	Total*	Pass	Comments
No universal default passwords	5	5/5	
Implement a means to manage reports of vulnerabilities	3	3/3	
Keep software updated	14	12/14	Optional requirement to allow the user to control the update has not been met.
Securely store sensitive security parameters	4	4/4	
Communicate securely	8	8/8	
Minimize exposed attack surfaces	9	9/9	
Ensure software integrity	2	2/2	
Ensure that personal data is secure	3	3/3	
Make systems resilient to outages	3	3/3	
Examine system telemetry data	1	1/1	
Make it easy for users to delete user data	4	4/4	
Make installation and maintenance of devices easy	3	3/3	
Validate input data	1	1/1	
Data protection provisions for consumer IoT	3	3/3	

**The total refers to the testing cases that are applicable in each evaluation.*

DEKRA Methodology

This section describes the criteria used by DEKRA when testing a product for compliance with the ETSI EN 303 645 following ETSI TS 103 701. 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 required forms (DuT Identification, ICS and IXIT) that the SO fills out to provide DEKRA with a detailed technical understanding of the product and its security controls.

The set of tests that were explicitly performed are detailed in the ETSI TS 103 701 document. This summary provides a broader perspective of the provisions included in ETSI EN 303 645 that DEKRA reviewed in alignment with the overall Google pledge.

1. No universal default passwords

Many consumer IoT devices are sold with universal default usernames and passwords (such as "admin, admin") for user interfaces through to network protocols. Continued usage of universal default values has been the source of many security issues in IoT devices and the practice needs to be discontinued.

2. Implement a means to manage reports of vulnerabilities

Device manufacturers need to make vulnerability disclosure policies publicly available. These policies must include a minimum framework to ensure safety and security for customers.

These minimum requirements are for contact information to be available for reporting issues, as well as providing information on timelines for receipt acknowledgements, and status updates until the issue is resolved.

3. Keep software updated

For IoT devices, it is important to keep the software regularly updated. This isn't just for performance enhancements of the device, but also for closing any vulnerabilities and ensuring the safety and security of the devices for the end user. Updates should be timely and verified for authenticity and integrity via a trust relationship.

4. Securely store sensitive security parameters

Provisioning a device with unique critical security parameters helps to protect the integrity and authenticity of software updates as well as the communication of the device with associated services. If global critical security parameters are used, their disclosure can enable wide-scale attacks on other IoT devices such as to enable the creation of botnets.

5. Communicate secure

Many different methods exist for a secure communication. Some authentication values are provided by out-of-band authentication mechanisms, such as a QR code, and some are human-readable, such as a password.

Where an authentication mechanism uses unique values per authentication attempt the response is not the authentication value itself.

6. Minimize exposed attack surfaces

The "principle of least privilege" is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application.

7. Ensure software integrity

The consumer IoT device should verify its software using secure boot mechanisms.

If a consumer IoT device detects an unauthorized change to its software, it will be able to inform the right stakeholder. In some cases, devices can have the ability to be in administration mode.

8. Ensure that personal data is secure

The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.

Also, all external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.

9. Make systems resilient to outages

The main aim is to ensure that IoT services are kept up and running as the adoption of IoT devices across all aspects of a consumer's life increases, including in functions that are relevant to personal safety.

It is important to note that safety-related regulations can apply, but the key is to avoid making outages the cause of impact on the user and to design products and services that provide a level of resilience to these challenges.

10. Examine system telemetry data

Examining telemetry, including log data, is useful for security evaluation and allows for unusual circumstances to be identified early and dealt with, minimizing security risk and allowing quick mitigation of problems.

11. Make it easy for users to delete user data

Consumer IoT devices often change ownership and will eventually be recycled or disposed of. Mechanisms can be provided that allow the consumer to remain in control and remove personal data from services, devices and applications. When a consumer wishes to completely remove their personal data, they also expect retrospective deletion of backup copies.

Deleting personal data from a device or service is often not simply achieved by resetting a device back to its factory default state. There are many use cases where the consumer is not the owner of a device, but wishes to delete their own personal data from the device and all associated services such as cloud services or mobile applications.

12. Make installation and maintenance of devices easy

Security issues caused by consumer confusion or misconfiguration can be reduced and sometimes eliminated by properly addressing complexity and poor design in user interfaces. Clear guidance to users on how to configure devices securely can also reduce their exposure to threats.

13. Validate input data

Systems can be subverted by incorrectly formatted data or code transferred across different types of interface.

Automated tools such as fuzzers can be used by attackers or testers to exploit potential gaps and weaknesses that emerge as a result of not validating data.

14. Data protection provisions for consumer IoT

Many consumer IoT devices process personal data. It is expected that manufacturers provide features within consumer IoT devices that support the protection of such personal data.

In addition, there exist laws and regulations that relate to the protection of personal data in consumer IoT devices (for example the GDPR). The present document intends to help manufacturers of consumer IoT devices provide a number of features for the protection of personal data from a strictly technical perspective.

Why DEKRA?

DEKRA has been ensuring safety since it was founded in 1925. This basic need is met with the extensive expertise, wide-ranging services, and passionate commitment of our workforce of more than 47,000 people in over 160 countries on all continents.

We have extended our vision to include security with regard to digitalization and connectivity. DEKRA has successfully accomplished a clear strategy to become the leading Test Laboratory for many technologies worldwide, and we are focused on 5 main areas: Automotive, Consumer, ICT, Industrial and Medical.

However, our mission goes far beyond these five areas. The company maintains a global and stable growth, promoting long-term alliances, customer's relationships, quality, talent, innovation and technology development.

This effort has resulted in the recognition by our clients and partners such as Amazon, BMW, Bosch, Belimo, etc.; industry alliances (GSMA, CSA, ioXt, GCF and CTIA) and standardization organizations (ETSI, ENISA, CEN, CENELEC, ISO, etc.).

Our experienced professional staff provides you with the expertise you need to ensure reliable functional cybersecurity. DEKRA - your global partner for a safe and secure world.