

ICS 35.240
CCS A 90

GA

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GA/T 1546-2019

**Information security technology - Security technical
requirements for WiFi signal monitoring products**

信息安全技术 无线WiFi信号监测产品安全技术要求

(English Translation)

Issued on: January 1, 1970

Implemented on: March 8, 2019

Issued by: Ministry of Public Security

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Wireless WiFi Signal Monitoring Product Description
5 General description
5.1 Classification of safety technical requirements
5.2 Classification of Security Levels.
6 Safety function requirements
6.1 Access point and terminal discovery
6.2 Positioning
6.3 Safety inspection
6.4 Whitelist
6.5 Identification and identification
6.6 Security management
6.7 Data security
6.8 Audit logs
7 Security requirements
7.1 Development
7.2 Guidance documents
7.3 Life cycle support
7.4 Testing
7.5 Vulnerability assessment
8 Requirements for different security levels
8.1 Safety Function Requirements
8.2 Security requirements

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard was proposed by the Cyber Security Bureau of the Ministry of Public Security.

This standard is under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security.

This standard was drafted. Computer Information System Security Product Quality Supervision and Inspection Center of the Ministry of Public Security, Network Security and Protection Bureau of the Ministry of Public Security.

1 Scope

This standard specifies the security function requirements, security guarantee requirements, and classification requirements for wireless WiFi signal monitoring products.

This standard applies to the design, development, and testing of wireless WiFi signal monitoring products.

2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 18336.3-2015 Information technology security technology Information technology security assessment guidelines Part 3. Security assurance components GB/T 25069-2010 Information Security Technology Terminology

3 Terms and definitions

GB/T 18336.3-2015 and GB/T 25069-2010 and the following terms and definitions apply to this document.

Wireless terminal

Network hardware devices, such as smart phones and laptops, that can access wireless access points via WiFi.

Wireless access point Allows wireless terminals to connect to wired networks or network hardware devices that form a wireless local area network, such as wireless routers, via WiFi.

WiFi signal monitoring product Monitor the wireless access points deployed in the information system and the WiFi signals of the wireless terminals connected to the wireless access points to obtain Wireless access point wireless terminal information product.

4 Wireless WiFi Signal Monitoring Product Description

Wireless WiFi signal monitoring products usually collect the WiFi signals of wireless access points and wireless terminals by wireless monitoring, and Line access point and wireless terminal information. Figure 1 is a typical operating environment for wireless WiFi signal monitoring products.

switch

Firewall router

server

Wireless access point Wireless WiFi Signal monitoring products Target network Wireless monitoring smart phone laptop Wireless WiFi communication

Figure 1 Typical operating environment of wireless WiFi signal monitoring products

5.1 Classification of safety technical requirements

This standard divides the security technical requirements of wireless WiFi signal monitoring products into two categories. security functions and security assurance requirements. Among them, safety Functional requirements are specific requirements for the security functions that wireless WiFi signal monitoring products should have; including access point and terminal discovery, positioning, Security detection, whitelisting, identification and authentication, security management, data security, audit logs; security assurance requirements for wireless WiFi signal monitoring Specific requirements are set for the life cycle process of the test product, including development, guidance documents, life cycle support, testing and vulnerability assessment.

5.2 Classification of security levels

The security level of wireless WiFi signal monitoring products is divided into basic level and enhanced according to the strength of its security function requirements and security assurance requirements.

Level, in which the security requirements refer to GB/T 18336.3-2015.

6.1.1 Access Point Information Acquisition

The product should be able to obtain the information of the monitored wireless access point, including SSID, MAC address, channel, encryption method, signal strength, connection Number of connected terminals.

6.1.2 Terminal Information Acquisition

The product should be able to obtain information about the wireless terminal connected to the monitored wireless access point, including the MAC address, device manufacturer, communication channel, Historical SSID and other information.

6.1.3 Hide SSID Access Point Discovery

The product should be able to monitor wireless access points with hidden SSIDs.

6.1.4 Monitoring method

The product should monitor wireless signals without access to the target network.

6.1.5 Monitoring frequency band

The product should support monitoring at least two signal bands. WiFi2.4G and WiFi5G.

6.1.6 Monitoring signal strength

The sensitivity of the product monitoring signal should be higher than -94dBm.

6.1.7 Statistics

The product should be able to count the instants of occurrence of the wireless access point being monitored and the number of occurrences over a period of time.

6.2 Positioning

The product should be able to locate the physical location of the wireless access point and determine its direction and distance.

6.3 Safety inspection

The product shall provide the following safety detection functions.

a) Authentication method detection. It can detect whether the authentication method of the wireless access point is safe;

b) Weak password detection. it can detect whether the wireless access point authentication password is a weak password;

Need to provide weak password library customization function;

c) Attack detection. It can detect whether the wireless access point is under attack.