NIST IR 8425 REPORT
GREE ASSESSMENT

GREE ELECTRIC APPLIANCES, INC. OF ZHUHAI
West Jinji Rd, Qianshan
519070 Zhuhai, Guangdong
People's Republic of China

Attn: Li Chunguang

REPORT NO
2161-048-D001

COMPILED BY
EWA-Canada, An Intertek Company

PROJECT NAME
GREE Smart Home Wifi Module: Models GRJWB05-J5 and GRJWB05-J10

DATE
22 November 2023

List of Revisions

REV.	DATE	REVISION DETAILS	AUTHOR	QA/REVIEW	APPROVED
1.0	22 November 2023	Final	CW	BC	SJ

Issuing office: Electronic Warfare Associates – Canada, Ltd., An Intertek Company ("Intertek")

Disclaimer

This report has been prepared for Gree Electric Appliances, Inc. of Zhuhai and should not be relied upon or used for any other project without an independent check being carried out as to its suitability and prior written authority of Intertek being obtained. Intertek accepts no responsibility or liability for the consequences of this document being used for a purpose other than the purposes for which it was commissioned. Any person using or relying on the document for such other purposes agrees and will by such use or reliance be taken to confirm his agreement to indemnify Intertek for all loss or damage resulting therefrom. Intertek accepts no responsibility or liability for this document to any party other than the person by whom it was commissioned.

EWA-Canada Locations

OTTAWA, ON

1223 Michael St. North,
Suite 200
Ottawa, Ontario, Canada
K1J 7T2

Tel (613) 230-6067
Fax (613) 230-4933

Executive Summary

Introduction

The client, Gree Electric Appliances, Inc. of Zhuhai, has produced Smart Home Wifi Module: Models GRJWB05-J5 and GRJWB05-J10, an independent communication module used to provide internet connectivity for other GREE products.

This report is intended to document that EWA-Canada has assessed the IoT product against the National Institute of Standards and Technology (NIST) Internal Report (IR) 8425 titled "Profile of the IoT Core Baseline for Consumer IoT Products" using client provided documentation and evidence.

Scope of Review

The IoT product assessed in this report is the Smart Home Wifi Module: Models GRJWB05-J5 and GRJWB05-J10. The NISTIR 8425 has two major sections that contain multiple capabilities. The scope of the assessment was based on those sections; the IoT Product Capabilities and IoT Product Developer Activities.

Results

Overall, GREE has provided the necessary information to EWA-Canada to score their device capabilities and their vendor activities against the NISTIR 8425. See Table 1 for a brief summary of the results score card and specific details can be seen in section 5.

Table 1 – NISTIR Summary of Score Card

NISTIR Results	
5.1 IoT Product Capabilities	**18/18**
5.2 IoT Product Developer Activities	**12/12**

The Smart Home Wifi Module: Models GRJWB05-J5 and GRJWB05-J10 produced by GREE has been scored against the IoT Product Capabilities section and has received a 18/18 score. The GREE activities has been scored against the IoT Product Developer Activities and has received a 12/12 score. A detailed results of the assessment please see the Results section of this report.

Table of Contents

List of Figures

List of Tables

1. Device Under Test

1.1 Testing Sponsor

Gree Electric Appliances, Inc. of Zhuhai

Contact: Li Chunguang
0756-8576232

Address: GREE ELECTRIC APPLIANCES, INC.
West Jinji Rd, Qianshan
519070 Zhuhai, Guangdong
Peoples Republic of China

1.2 Configuration Details

Manufacturer:	Gree Electric Appliances, Inc. of Zhuhai
Product name:	Smart Home Wifi Module: Models GRJWB05-J5 and GRJWB05-J10
Model Number:	GRJWB05-J5 and GRJWB05-J10
Device Class:	Electrical
Document Review date:	22 November 2023

1.3 Testing Participants

Report Author:	Chris Wilson
Technical Reviewer:	Ben Cuthbert
Releasing Officer:	Steve Jia

2. INTRODUCTION

2.1 Background

The client, Gree Electric Appliances, Inc. of Zhuhai, has produced Smart Home Wifi Module: Models GRJWB05-J5 and GRJWB05-J10, an independent communication module used to provide internet connectivity for other GREE products.

This report is intended to document that EWA-Canada has assessed the IoT product against the National Institute of Standards and Technology (NIST) Internal Report (IR) 8425 titled “Profile of the IoT Core Baseline for Consumer IoT Products” using client provided documentation and evidence.

2.2 Scope

The IoT product assessed in this report is the Smart Home Wifi Module: Models GRJWB05-J5 and GRJWB05-J10 Smart Home Wifi Module: Models GRJWB05-J5 and GRJWB05-J10. The scope of assessment is based on the two sections with in the NISTIR; the IoT Product Capabilities and IoT Product Developer Activities.

2.3 Disclaimer

This report is intended to document that EWA-Canada has made the best possible effort using the most current tools, technology, and methods as well as using skilled security testers to identify as many security issues as possible within the scope of the engagement at the time of testing. Cyber security threats are continuously changing, and no application or system can ever be considered 100% secure regardless of how much security testing is conducted.

2.4 References

[1] Intertek NIST IR 8425 - Test Plan v1.0

[2] EWA-Canada Quote: 23874-225-002 *Quote to Conduct a Cyber Security Review for the IoT Devices based on NIST IR 8425*

[3] NISTIR 8425, September 2022

3. System Description

The Gree Electric Appliances, Inc. of Zhuhai Smart Home Wifi Module – models GRJWB05-J5 and GRJWB05-J10 are the independent communication modules used in GREE's household electric appliances.

Figure 1 – Smart Home Wifi Module: Models GRJWB05-J5 and GRJWB05-J10

3.1 System Components

GREE Smart Home Wifi Modules Model GRJWB05-J5 and GRJWB05-J10 work with a cloud service and a mobile application.

- Smart Home Wifi Module – Model GRJWB05-J5 or GRJWB05-J10
- Android Application – GREE+ 1.18.0
- Apple Application – GREE+ 1.18.0

4. METHODOLOGY

This section describes the methodology used to perform each of the required tasks as well as the rationale behind the score ratings.

4.1 Documentation review

EWA-Canada conducted the documentation review as described in the quote which was based on client provided documentation for each item of the NISTIR. The client was requested to provide documentation demonstrating adherence to the capabilities outlined in the NISTIR 8425. The purpose of this review was to gather essential information about the IoT product and score it against each item in the NISTIR 8425.

4.2 Score Ratings

In order to provide justification to each score rating a score rating classification key is provide below.

Table 2 – Score Rating Classification Key

SCORE RATING CLASSIFICATION KEY	
Classification	**Description**
3/3	The vendor has successfully implemented the capability or is effectively following the activity.
2/3	The vendor has mostly implemented the capability or is reasonably following the activity.
1/3	The vendor has partially implemented the capability or is somewhat following the activity.
0/3	The vendor has not started to implement the capability or has not started to follow the activity.

5. RESULTS

This section documents the results of the security testing including any issues observed and indicates all conformances and non-conformances to the capabilities.

5.1 IoT Product Capabilities

5.1.1 Asset Identification

The IoT product is uniquely identifiable and inventories all of the IoT product's components.

Score: 3/3
Evidence: The product is uniquely identifiable due to the labeled brand, model number, and serial number. The mobile application keeps an inventory of the IoT device and relies on the unique MAC address. Once a device is provisioned to a user's account, an inventory of the user's products can be seen in the mobile application.

5.1.2 Product Configuration

The configuration of the IoT product is changeable, there is the ability to restore a secure default setting, and any and all changes can only be performed by authorized individuals, services, and other IoT product components.

Score: 3/3
Evidence: Product configuration can be changed by authorized persons, in this case only the vendor. The ability exists for the main user to restore the product. The process taken by the product when a configuration change is made was established.

5.1.3 Data Protection

The IoT product protects data stored across all IoT product components and transmitted both between IoT product components and outside the IoT product from unauthorized access, disclosure, and modification.

Score: 3/3
Evidence: Password and certificate information is stored in folders that only the APP has permission to access and are encrypted using AES-128 while in use. Communications are encrypted using AES-128 as well.

5.1.4 Interface Access Control

The IoT product restricts logical access to local and network interfaces – and to protocols and services used by those interfaces – to only authorized individuals, services, and IoT product components.

Score: 3/3
Evidence: Only the ports needed for the product's function are left open. Access to the product is limited to those with provisioned accounts, using their credentials. Commands are sent over TLS and encrypted using AES-128.

5.1.5 Software Update

The software of all IoT product components can be updated by authorized individuals, services, and other IoT product components only by using a secure and configurable mechanism, as appropriate for each IoT product component.

Score: 3/3
Evidence: Customer is prompted by the APP when an update is available, and the update is securely transferred using encrypted traffic and SHA-256 values are verified.

5.1.6 Cybersecurity State Awareness

The IoT product supports detection of cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.

Score: 3/3
Evidence: Amazon Cloudwatch services are used to monitor the state of IoT components. Protected data is not stored within the product's logs. When a change is made to the device the main user is notified through the APP.

5.2 IoT Product Developer Activities

5.2.1 Documentation

The IoT product developer creates, gathers, and stores information relevant to cybersecurity of the IoT product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.

Score: 3/3
Evidence: The seven sub-sections (from a to g) are addressed within the product documentation provided.

5.2.2 Information & Query Reception

The IoT product developer has the ability to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.

Score: 3/3
Evidence: Proper vulnerability reporting channels are in place. Feedback can be sent to the vendor from the APP, an email address has also been provided.

5.2.3 Information Dissemination

The IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.

Score: 3/3
Evidence: Relevant information is posted on listed websites, while customers are notified through a mixture of OTA updates and email. Time periods for maintenance, life of product and support clearly defined. Certificates and other relative information shipped with product.

5.2.4 Product Education & Awareness

The IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the IoT product and its product components.

Score: 3/3
Evidence: Education and awareness documentation satisfies the listed requirements. All relevant information needed by a customer is present.

6. SUMMARY OF RESULTS

Gree Electric Appliances, Inc. of Zhuhai has presented evidence for each item evaluated in the NISTIR, resulting in score ratings that are included in Table 3 – NISTIR Score Card.

Table 3 – NISTIR Score Card

NISTIR Results	
5.1 IoT Product Capabilities	**18/18**
5.1.1 Asset Identification	**3/3**
5.1.2 Product Configuration	**3/3**
5.1.3 Data Protection	**3/3**
5.1.4 Interface Access Control	**3/3**
5.1.5 Software Update	**3/3**
5.1.6 Cybersecurity State Awareness	**3/3**
5.2 IoT Product Developer Activities	**12/12**
5.2.1 Documentation	**3/3**
5.2.2 Information & Query Reception	**3/3**
5.2.3 Information Dissemination	**3/3**
5.2.4 Product Education & Awareness	**3/3**