SB-327 (CALIFORNIA IOT) ASSESSMENT REPORT
TWINKLY LED LIGHTS

TWINKLY

REPORT NO
2161-010-D001

COMPILED BY
EWA-Canada, An Intertek Company

PROJECT NAME
Twinkly LED Lights

DATE
10 November 2020

List of Revisions

REV.	DATE	REVISION DETAILS	AUTHOR	QA/REVIEW	APPROVED
1.0	09 April 2020	Final	SE	NL/SJ	SJ
1.1	13 April 2020	Model numbers update	SE	NL/SJ	SJ
1.2	20 April 2020	Image Updates	NL	SJ	SJ
1.3	09 November 2020	Model Update	SE	NL	SJ
1.4	10 November 2020	Minor Edit	SJ	SJ	SJ

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

Disclaimer

EWA-Canada Locations

OTTAWA, ON	ST. JOHN'S, NL
1223 Michael St. North, Suite 200 Ottawa, Ontario, Canada K1J 7T2 Tel (613) 230-6067 Fax (613) 230-4933	139 Water St., Suite 601 St. John's, Newfoundland, Canada A1C 1B2 Tel (709) 726-0667 Fax (709) 726-0668

EXECUTIVE SUMMARY

Introduction

The client, Twinkly, has developed a product named Twinkly LED Lights.

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 this report should be considered a snapshot of security in time.

Scope of Review

The product assessed in this report is the Twinkly LED Lights. The scope of testing is based on the following cyber requirements specified in SB-327 ("The California IoT Bill"):

a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:
    1. Appropriate to the nature and function of the device.
    2. Appropriate to the information it may collect, contain, or transmit.
    3. Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.
b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:
    1. The pre-programmed password is unique to each device manufactured.
    2. The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

Intertek has derived test cases from these requirements which were used to assess these products.

Results

Twinkly has provided a reasonable level of security appropriate to the function of the device. No unexpected services have been found to be actively listening on the Twinkly LED Lights.

The following table summarizes the results of the tests that were performed in accordance with the derived test requirements designed to comply with SB-327. Full details of the test methodologies and results are contained in the report.

Table 1– SB-327 Summary of Results

SB-327 Derived Test Case Results	
1. Product Installation	PASS
2. Default Password	PASS
3. Manufacturers Attestation	PASS
4. Sensitive Information	PASS
5. Data Flows	PASS
6. Communications	PASS
7. Unexpected Communications	PASS
8. Bluetooth Communications	PASS
9. IP Communications	PASS
10. Active Services	PASS
11. Automated Vulnerability Assessment	PASS
12. Software/Firmware Update	PASS

As a result of testing, the Twinkly LED Lights, produced by Twinkly, has met all test cases designed to meet the requirements of the “California IoT Bill” SB-327.

Table of Contents

List of Figures

List of Tables

1 INTRODUCTION

1.1 Background

The client, Twinkly, has developed a product named Twinkly LED Lights.

1.2 Purpose

The purpose of this testing was to test the products against requirements which were derived by Intertek in order to test suitability of connected products against the “California IoT Bill”, SB-327.

1.3 Scope

The products assessed in this report is the Twinkly LED Lights. The scope of testing is based on the following cyber requirements specified in SB-327 (“The California IoT Bill”):

a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:
    1. Appropriate to the nature and function of the device.
    2. Appropriate to the information it may collect, contain, or transmit.
    3. Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:
    1. The pre-programmed password is unique to each device manufactured.
    2. The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

Intertek has derived test cases from these requirements, which were used to assess these products.

1.4 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.

1.5 References

[1] California Legislative Information, *Senate Bill No. 327,* available online: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327, September 2018.

[2] EWA-Canada Quote: 20874-072-016- Quote to Conduct a Cyber Security Review for the Twinkly LED Lights based on California Senate Bill No. 327”, October 10, 2020

2 SYSTEM DESCRIPTION

The Twinkly LED Lights, produced by Twinkly, uses Bluetooth Low Energy for setup; default state is disabled. By pressing and holding the button on the controller for 5 sec, the LED status indicator turns light blue and the Bluetooth connectivity is enabled. During this phase, the device is visible, and the mobile application can connect to the device. The only functions available via Bluetooth are related to entering Wi-Fi credentials in order to let the controller establish a connection to the local Wi-Fi. The LED lights allows for remote control using a phone.

Figure 1 – Twinkly LED Lights

Figure 2 - Multiport Controller

Figure 3 - Multiport Controller Board

Figure 4 -PCB: LWS-TW6 Double Port Controller Board

The testing in this report is focused on the PGT750STP, PGT750SPP and TWS400STP models. The vendor confirmed that the following models listed below are very similar to the models that were tested. The other models included are as follows:

Table 1 – Twinkly Model numbers

No.	ITEM P/N	DOUBLE PORT CONTROLLER LWS-TW3	4 PORT CONTROLLER LWS-ML2	2 PORT CONTROLLER LWS-TW6
1	TWS100STP-xxx	x		
2	TWS250STP-xxx	x		
3	TWS400STP-xxx	x		
4	TWS600STP-xxx	x		
5	TWS250SPP-xxx	x		
6	TWS400SPP-xxx	x		
7	TWS250GOP-xxx	x		
8	TWS400GOP-xxx	x		
9	TWI190STP-xxx	x		
10	TWI190SPP-xxx	x		
11	TWI190GOP-xxx	x		
12	TWW210SPP-xxx	x		
13	TWB200STP-xxx	x		
14	TWC400STP-xxx	x		
15	TWC400GOP-xxx	x		
16	TWT500STP-xxx	x		
17	TWT500GOP-xxx	x		
18	TWT400SPP-xxx	x		
19	TWT400STP-xxx	x		
20	TWT400GOP-xxx	x		
21	TWT250STP-xxx	x		
22	TWT250GOP-xxx	x		
23	TWR050SPP-xxx	x		
24	TWG050SPP-xxx	x		
25	TWF020STP-xxx	x		
26	PGT750STP		x	
27	TW-TBCxxx-yyyy*		x	x
28	PGS400STP	x		
29	PGS250STP	x		
30	PGS250GOP	x		
31	PGS150STP	x		
32	PGS150GOP	x		
33	PGS100STP	x		
34	PGS100GOP	x		
35	PGS050STP	x		
36	PGS050GOP	x		
37	PGI190STP	x		
38	PGI050GOP	x		
39	PGT750SPP		x	

*note: xxx indicates the controller version, can be 0-9, A-Z or blank, yyyy indicates the LED numbers