LYNS-TCi

CYBERSECURITY ASSESSMENT TEST REPORT

PSTI TEST

Test report Nº.: HC2407190100GC02

Issued date: 2024-10-28

Prepared by:

Unicorn

Unicorn Zhang / Test engineer

Approved by

LYNS-TCi TECHNOLOGY
LYNS-TCi

Lukes

Lukes Lin / Projection manager

Table of Content

1 REPORT HISTORY

1.1 Report Revision History

Client	Date	Change Description	Validity
EAST	2024-10-28	Final	Valid

1.2 Report Template Revision History

Date	Version	Comments	Changed by	Approved by
2023/11/20	Rev1	Creation	Case	Genk

2 Terms and Conditions

The test results presented in this report relate only to the object tested.

This report is for the exclusive use of Lyns-tci Technology Guangdong Co., Ltd. (abbreviation: Lyns-tci) Client and is provided pursuant to the agreement between Lyns-tci and its Client. This report shall not be reproduced, except in full, without the written approval of Lyns-tci. Test reports without seal and signature are not valid.

Lyns-tci responsibility and liability are limited to the terms and conditions of the agreement. Lyns-tci assumes no liability to any party, other than to the Client in accordance with the agreement, for any loss, expense or damage occasioned using this report.

Information on derived or extended models of the range as provided by the applicant (if any) is included in this report for information purposes only. Lyns-tci shall not be liable for any incorrect results due to unclear, incorrect, incomplete, misleading or false information provided by client.

3 INTRODUCTION

3.1 Scope & Methodology

This test report is based on the testing, evaluation, and judgment of the 5.1-1/5.1-2/5.2-1/5.3-13 in ETSI EN 303 645 mentioned in UK "The Product Security and Telecommunications Infrastructure (Security Requirements for Reliant Connected Products) Regulations 2023", in order to provide relevant reference information for the compliance of the tested cyber attribute products.

3.2 References

Document	Date	Version	Comments
ETSI EN 303 645	2020-06	V2.1.1	Cyber Security for Consumer Internet of Things: Baseline Requirements
ISO/IEC 29147	2018	/	
The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023			

4 TARGET OF EVALUATION

The target of evaluation for this assessment is the IoT device including it’s interfaces and interactions with associated services.

As input to the assessment the manufacturer has provided information in the form of an Implementation Conformance Statement (ICS) and extra Information for Testing (IXIT). The proforma is defined by ETSI.

Additionally samples of the Device under Test (DUT) have been provided by the manufacturer to the Lyns-tci Technology Guangdong Co., Ltd.

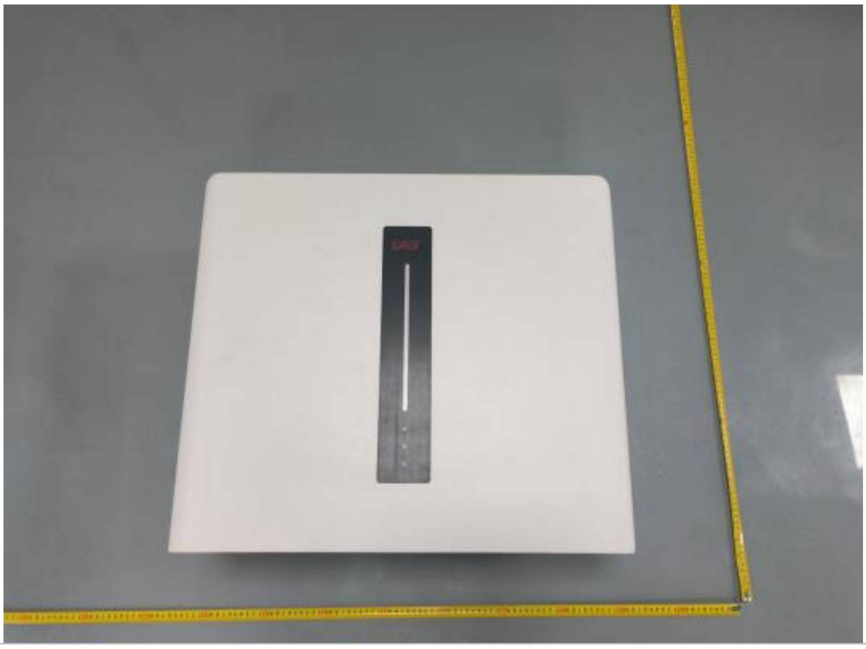
4.1 Manufacturer Contact Information

Information	Manufacturer
Company Name	EAST Group Co., Ltd.
Address	No.6 Northern Industry Road, Songshan Lake Sci. & Tech. Industrial Park, Dongguan City, Guangdong Province, China
Contact	Haijian Pan, renzheng@eastups.com

4.2 Device Under Test (DUT)

Information	Manufacturer
Product Name	Converter（Hybrid Inverter with storage battery system）
Type or Model	EAHI-6000-SL-S
System & Firmware Version	DSP1036 MCU1035
Hardware Version/ Batch No.	V1.0
Intended App & version	iServiceTool-SUN:V1.1.2 IECloud:V1.3.405
Device features	RS485/WIFI

Foto(s) of the DUT

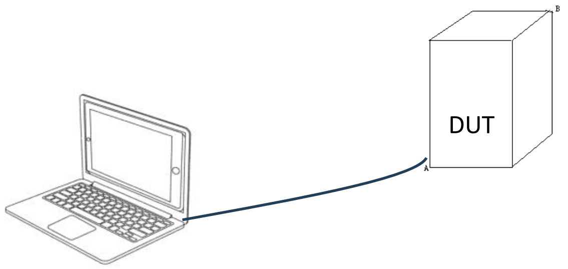


5 TEST SETUP

The test setup consists of the DUT, auxiliary equipment, test equipment and test software tools. It is operated by the test lab and provides the environment in which the DUT is assessed.

The test equipment and test software tools are provided, maintained and are used by the test lab to execute the test procedures.

Architecture of the Test Setup



5.1 Test Equipment

Test Equipment used during the assessment			
Device Name	**Function**	**Manufacturer**	**Version**
computer test system	Testing environment integrity	Lenovo M710s	/

6 ASSESSMENT RESULTS

6.1 Overview

- “**PASS**” verdict is assigned when the required elements for the test case performance are present; and the criteria for pass defined for each test step in the "Assignment of Verdict" are fulfilled.
- “**FAIL**” verdict is assigned when the required elements for the test case performance are present; and the criteria for fail defined for one of the test steps in the "Assignment of Verdict" are fulfilled.
- “**INCON**” = “Inconclusive” verdict is assigned when the required elements (e.g. evaluation tools and IXIT information) for the test case performance are not present or are not sufficient to allow a proper execution of the test case and therefore no meaningful pass or fail verdict can be assigned.
- “**N/E**” is assigned when the tester lab has **not evaluated** the requirement. This can be the case if the manufacturer answered in the ICS the Support = Not supported (N) or Not applicable (N/A).
- “**-**“ means

6.2 Summary

Provision	**Description**	**Verdict**
No universal default passwords		
5.1-1	Unique per device passwords	PASS
5.1-2	Pre-installed password randomness	PASS
Implement a means to manage reports of vulnerabilities		
5.2-1	vulnerability disclosure policy publicly	PASS
Keep software update		
5.3-13	Product support	PASS

-

6.2.1 No universal default passwords

The password **must be**
(a) Each product is unique; Or (b) defined by the product user.

The unique password for each product **must not be**
(a) Based on an up counter;
(b) Based on or derived from public information;
(c) Based on or derived from unique product identifiers, such as serial numbers, unless encryption methods or key hashing algorithms are used, which is recognized as part of good industry practice;
(d) As part of good industry practice, make guesses in an unacceptable manner.

The password **must** not contain
(a) Key;
(b) Personal identification numbers used for pairing in communication protocols that do not form part of the Internet Protocol Suite; or
(c) Application programming interface key.

Test Case 5.1-1	
PROVISION 5.1-1	Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.
Assignment of verdict	The verdict **PASS** is assigned if: - Each password of a password-based authentication mechanism being used in any state other than the factory default, that is not defined by the user, is unique per device. The verdict **FAIL** is assigned otherwise. The verdict **PASS** is assigned if: • Every discovered password-based authentication mechanism is documented in the IXIT; **AND** • The user is required to define all passwords before being used, that are stated as defined by the user in the IXIT **AND** • There is no indication that the generation of a not user-defined password of the DUT used in any state other than the factory default differs from the generation mechanism described in the IXIT. The verdict **FAIL** is assigned otherwise

Test Result	
Testlab Comments	**Verdict**
The device provides login interfaces through user APP and WEB, using the same and only user ID (account). Each device can only be bond to one user ID, which requires a unique password.	PASS

Test Case 5.1-2	
PROVISION 5.1-2	Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device..
Assignment of verdict	The verdict **PASS** is assigned if: - No obvious regularities in pre-installed passwords is found; **AND** - No common strings or other common patterns in pre-installed passwords is found; **AND** - The generation mechanisms for pre-installed passwords do not induce passwords, That are related in an obvious - way to public information; **AND** - The generation mechanisms for pre-installed passwords are considered appropriate in terms of complexity The verdict **FAIL** is assigned otherwise The verdict **PASS** is assigned if: - Meet the requirements of 5.1-1 - for each pre-installed password there is no indication, that its generation differs from the generation mechanism described in the IXIT. The verdict **FAIL** is assigned otherwise.

Test Result

Testlab Comments	Verdict
The device provides login interfaces through user APP and WEB, using the same and only user ID (account). Each device can only be bond to one user ID, which requires a unique password. No password generator is used.	**PASS**

6.2.2 Implement a means to manage reports of vulnerabilities

The following information must be disclosed -

(a) At least one contact information that allows personnel ("P") to report safety issues to the manufacturer

(b) When will P receive it

(i) Confirm receipt of security issue report;

(ii) Update the status until the reported security issue is resolved.

The information must be accessible, clear and transparent, and must be provided to P -

(a) And there is no need to request such information in advance;

(b) English;

(c) Free of charge;

(d) And not requiring the provision of P's personal information.

TC_VULNERABILITY_REPORTING#1 / Test case 5.2-1-1	
Security requirement	PROVISION 5.2-1

TC_VULNERABILITY_REPORTING#1 / Test case 5.2-1-1	
Documentation analysis objectives	Verify that vulnerability disclosure policy publication is available to anybody
Evaluation inputs	**“Publication of vulnerability disclosure”**,e.g.Website links
Documentation analysis procedure	Do a short analysis of the vulnerability disclosure policy publication (for instance referring to **ISO/IEC 29147(2018) clause 6.2**). a) Tester access to the publication as described i.e. whether anybody can access the documentation. b) Tester do a short analysis of the **vulnerability disclosure policy publication** Tester check whether in the user manual and in the information’s bonded to the device that vulnerability disclosure policy contains - Contact information Information about timelines regarding acknowledgement of receipt and status updates
Verdict	The verdict PASS is assigned if: - Publication of the vulnerability disclosure policy is available to anybody The verdict FAIL is assigned otherwise. The verdict PASS is assigned if: - The vulnerability disclosure policy is publicly accessible; **AND** - The vulnerability disclosure policy contains contact information and information on timelines regarding acknowledgement of receipt and status updates. The verdict FAIL is assigned otherwise.

Test Result	
Comments	**Verdict**
EAST has released its vulnerability disclosure policy webpage at the following link: http://3.75.93.227:8080/#/security The contact person is: psirt@eastups.com	PASS

6.2.3 Keep software update

The determined support period must be announced.

If the manufacturer extends the minimum time for providing security updates and creates a new confirmed support period, new confirmed support must be released as soon as feasible.

The information must be accessible, clear and transparent, and must be provided to P -

(a) And there is no need to request such information in advance;
(b) English;
(c) Free of charge;
(d) And not requiring the provision of P's personal information.
(e) In a way that readers can understand without prior technical knowledge.

If the determined support period is shortened after the information is released, it does not meet the security requirements in this clause

TC_SOFTWARE_UPDATE_#16 / Test case 5.3-13-1	
Security requirement	PROVISION 5.3-13
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the publication of the defined support period.
Documentation analysis procedure	The tester shall assess whether access to the **"Publication of Support Period"** is understandable and comprehensible for a user with limited technical knowledge.
Verdict	The verdict PASS is assigned if: • The publication of software update support period is understandable and comprehensible for a user with limited technical knowledge. The verdict FAIL is assigned otherwise. The verdict PASS is assigned if: • The access to the resource for publishing the defined support period to the user is provided as described • The access to the resource for publishing the defined support period is unrestricted **AND** • The defined support period is published. The verdict FAIL is assigned otherwise.

Test Result	
Comments	**Verdict**
EAST has announced the software upgrade support period at the following link: http://3.75.93.227:8080/#/security - guarantee period: September 27, 2033	PASS