

TEST REPORT PPP 17004A: 2020 TÜV SÜD Test Report for IoT Consumer products – Cybersecurity – European market	
Report No.:	6818922034901
Date of issue:	2023-04-18
Project handler:	Buddy He
Testing laboratory:	TÜV SÜD Certification and Testing (China) Co., Ltd. Shenzhen Branch
Address:	Building 12 & 13, Zhiheng Wisdomland Business Park, Nantou Guankou Erlu, Nanshan District Shenzhen 518052, P.R. China.
Testing location:	as above
Client:	Jackery Technology GmbH
Client number:	120814
Address:	Hahnstraße 70 60528 FRANKFURT GERMANY
Contact person:	Ricky Ma
Standard:	This TÜV SÜD test report form is based on the following requirements: ETSI EN 303 645 V2.1.1:2020-06
TRF number and revision:	TRF_ PPP 17004A:2020 rev. 1.1:2021
TRF originated by:	TÜV SÜD Product Service, Mr. Roland Fiat (<i>senior product specialist</i>)
Copyright blank test report:	This test report is based on the content of the standard (see above). The test report considered selected clauses of the a.m. standard(s) and experience gained with product testing. It was prepared by TÜV SÜD Product Service. TÜV SÜD Group takes no responsibility for and will not assume liability for damages resulting from the reader's interpretation of the reproduced material due to its placement and context.
General disclaimer:	This test report may only be quoted in full. Any use for advertising purposes must be granted in writing. This report is the result of a single examination of the object in question and is not generally applicable evaluation of the quality of other products in regular production.
Scheme:	☐ TÜV Mark ☒ without certification Non-standard test method: ☒ No ☐ Yes, see details under Summary of testing National deviations: N/A
Number of pages (<i>Report</i>):	13
Number of pages (<i>Attachments</i>):	11 pages for Attachment No.1
Compiled by: Buddy He (+ signature) 	Approved by: Homer Zhong (+ signature) 

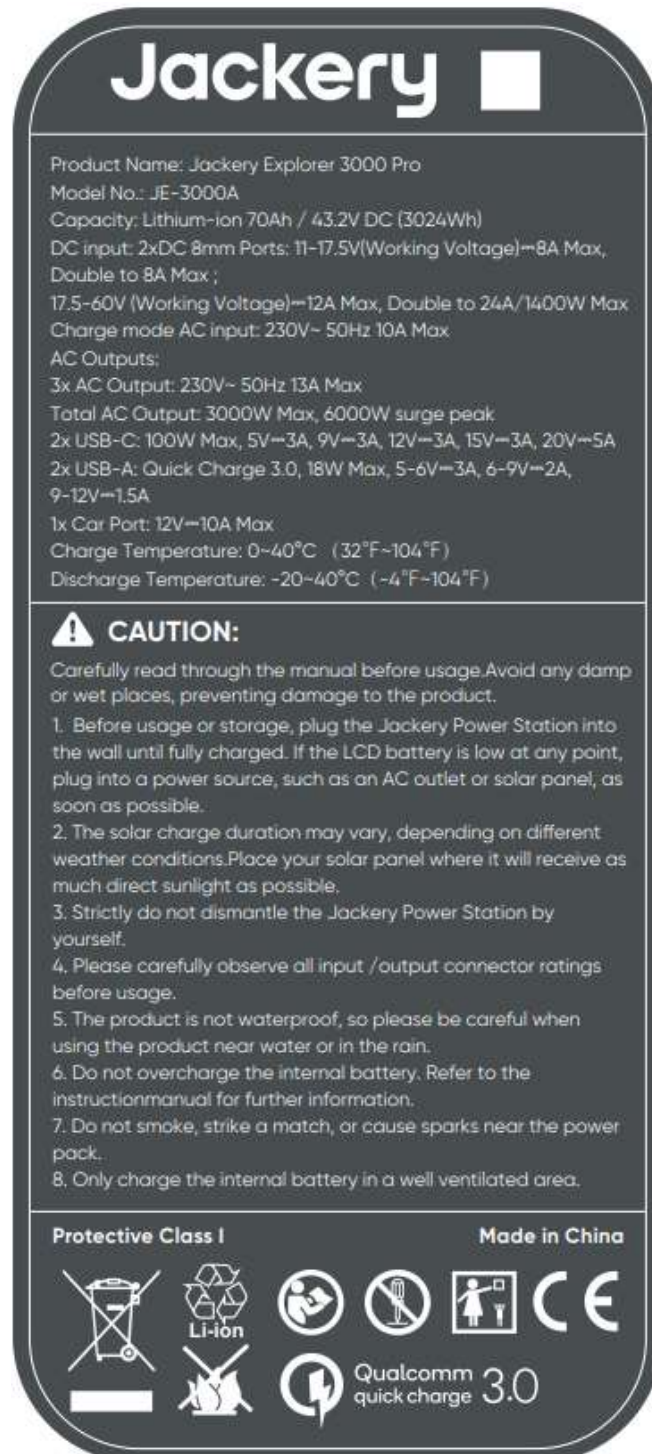


Attachments:	
Attachment No.1:	
Photo document of the Item Tested.	
Considering security of report, we do not attach self-declaration document.	
Test sample:	Mass production sample
Type of test object:	Power Station
Trademark:	
Model and/or type reference:	JE-3000A, JE-2000C, JE-1000B, JE-1000C, JE-300B
Parameters:	Wi-Fi and BLE module model: ESP32-C3-MINI-1 Wi-Fi and BLE module firmware version: V2.4.2 Wi-Fi and BLE module OS version: FreeRTOS V10.4.3 Main control board model: Refer to Appendix 1 Main control board firmware version: Refer to Appendix 1 Main control board PCB version: Refer to Appendix 1 Main control Soc chip: GD32F303
Manufacturer:	Shenzhen Hello Tech Energy Co.,Ltd.
Manufacturer number:	002386
Address:	F2-3 Bldg.7, Jiaanda Science and Technology Industrial Park Factory, the East Side of Huafan Road, Tongsheng Community, Dalang Street, Longhua District, Shenzhen, Guangdong, PEOPLE'S REPUBLIC OF CHINA
Sub-contractors/ tests (clause):	N/A
Name:	N/A
Order description:	☒ Complete test according to TRF ☐ Partial test according to manufacturer's specifications ☐ Preliminary test ☐ Spot check ☐ Others:
Date of order:	2022-12-07
Date of receipt of test item:	2023-01-17
Date(s) of performance of test:	2023-02-06~2023-03-08
Test item particulars:	
Device features:	
- Sensors	N/A
- Actuators	N/A

ID: ENE-R&D_GCN_F_01.01E - Rev.00 - Effective date: 16 Nov 2021
Created by: Stone Zhong Released by: Jerry Tang

- Human user interfaces	Physical buttons, Buzzer
- Communication interfaces	Wi-Fi (802.11 b/g), Bluetooth LE 5.0
- Local interfaces	2 USB Type-C (for charging), 2 USB Type-A (for charging), other AC input and output interfaces
Software versions:	
- Android IoT app versions	Jackery 1.0.0
- iOS IoT app versions	Jackery 1.0.0
- Firmware/software versions	Wi-Fi and BLE module firmware version: V2.4.2 Wi-Fi and BLE module OS version: FreeRTOS V10.4.3
Purpose of the product (Description of intended use): The Jackery Explorer is a solar-ready portable power station designed to provide the power you need for mobile living and outdoor life.	
Characteristic data (not shown on the marking plate): N/A	

Copy of the marking plate



JE-3000A is chosen as the representative model.

For other models' marking plates, please refer to Attachment 1.

Picture of the product:



JE-3000A is chosen as the representative model.

For other models' pictures, please refer to Attachment 1.

Summary of testing:

Unless otherwise specified, the model JE-3000A is chosen as the representative model to perform all the test.

Additional models were added, please refer to detail below:

1. All additional models have the same cybersecurity related elements including Wi-Fi module, local interface, communication mechanism, mobile application, security policy for vulnerability management as JE-3000A. The differences are mainly in aspects such as circuit diagram, PCB layout, BOM, appearance, mechanical construction, which are irrelevant with cybersecurity.
2. Critical security parameters are stored within the device, which is same as the representative model JE-3000A.
3. All product models use the same mobile applications - Jackery 1.0.0 (Android&iOS).

The samples declared were found to comply with ETSI EN 303 645 V2.1.1:2020.

The submitted samples were found to comply with the above specification.

- ☐ deviation(s) found
☒ no deviations found

Additional information on non-standard test method(s)

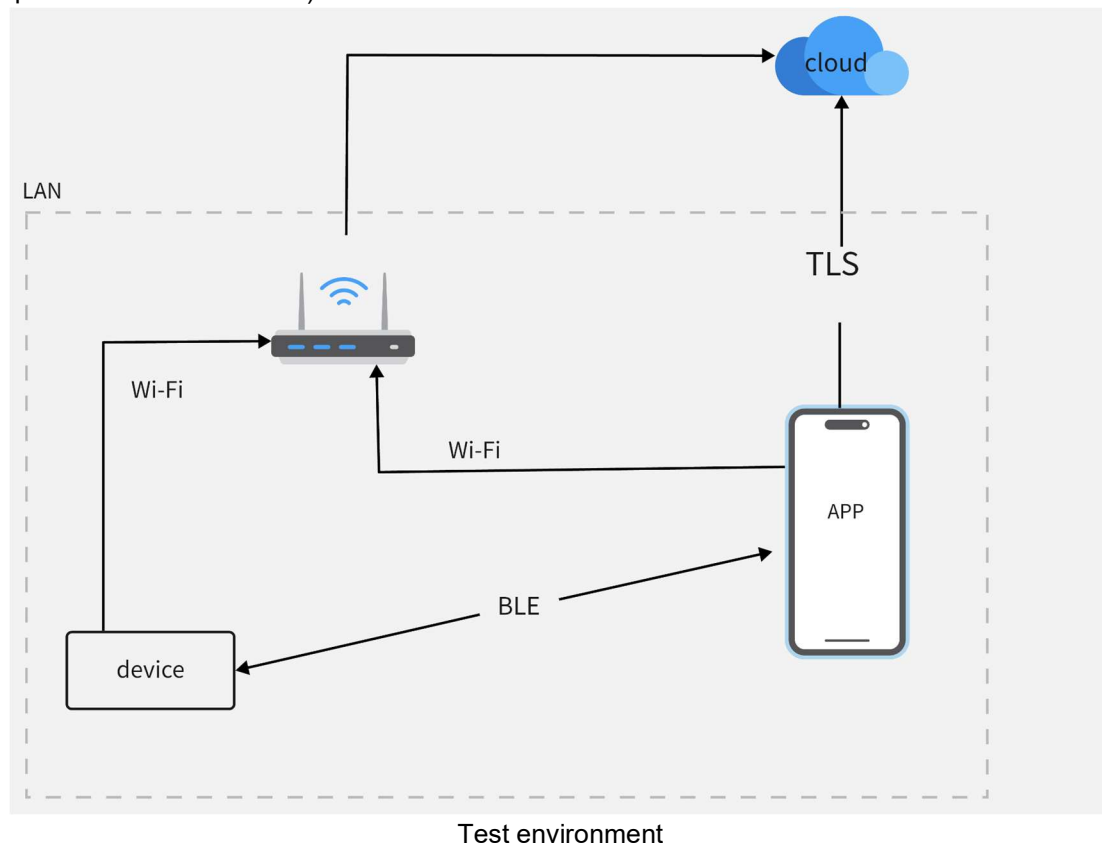
Sub clause: None
Page: N/A
Rationale: N/A

If additional information is necessary, please provide. N/A

Possible test case verdicts:
- test object does meet the requirement: P (Pass)
- test object does not meet the requirement: F (Fail)
- test case does not apply to the test object: N/A (Not applicable)
Possible suffixes to the verdicts:
- suffix for detailed information for the client: C (Comment)
- suffix for important information for factory inspection: M (Manufacturing)

Test Environment

(Description of test environment)



Clause	Requirement + Test	Remark	Verdict
4	Reporting implementation		/
4-1	(M) A justification shall be recorded for each recommendation in the present document that is considered to be not applicable for or not fulfilled by the consumer IoT device.		P
5	Cyber security provisions for consumer IoT		/
5.1	No universal default passwords		/
5.1-1	(MC) 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.	There is no authentication mechanism for the device to verify the user.	N/A
5.1-2	(MC) 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.	There is no authentication mechanism for the device to verify the user.	N/A
5.1-3	(MC) Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.	There is no authentication mechanism for the device to verify the user.	N/A
5.1-4	(MC) Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.	There is no authentication mechanism for the device to verify the user.	N/A
5.1-5	(MC) When the device is not a constrained device, it shall have a mechanism available which makes brute-force attacks on authentication mechanisms via network interfaces impracticable.		P
5.2	Implement a means to manage reports of vulnerabilities		/
5.2-1	(M) The manufacturer shall make a vulnerability disclosure policy publicly available.		P
5.2-2	(R) Disclosed vulnerabilities should be acted on in a timely manner.		P
5.2-3	(R) Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period.		P
5.3	Keep software updated		/
5.3-1	(R) All software components in consumer IoT devices should be securely updateable.		P
5.3-2	(MC) When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.		P
5.3-3	(MC) An update shall be simple for the user to apply.		P
5.3-4	(RC) Automatic mechanisms should be used for software updates.	The device doesn't support automatic updates. Software updates require user consent.	N/A

Clause	Requirement + Test	Remark	Verdict
5.3-5	(RC) The device should check after initialization, and then periodically, whether security updates are available.		P
5.3-6	(RC) If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications.	The device doesn't have an ability to configure automatic updates and update notifications.	N/A
5.3-7	(MC) The device shall use best practice cryptography to facilitate secure update mechanisms.		P
5.3-8	(MC) Security updates shall be timely.		P
5.3-9	(RC) The device should verify the authenticity and integrity of software updates.		P
5.3-10	(MC) Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.		P
5.3-11	(RC) The manufacturer should inform the user in a recognisable and apparent manner that a security update is required together with information on the risks mitigated by that update.		P
5.3-12	(RC) The device should notify the user when the application of a software update will disrupt the basic functioning of the device.		P
5.3-13	(M) The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.		P
5.3-14	(RC) For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user.	The device is not a constrained device.	N/A
5.3-15	(RC) For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.	The device is not a constrained device.	N/A
5.3-16	(M) The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.		P
5.4	Securely store sensitive security parameters		/
5.4-1	(MC) Sensitive security parameters in persistent storage shall be stored securely by the device.		P
5.4-2	(MC) Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.		P
5.4-3	(M) Hard-coded critical security parameters in device software source code shall not be used.		P
5.4-4	(MC) Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.		P
5.5	Communicate securely		/
5.5-1	(M) The consumer IoT device shall use best practice cryptography to communicate securely.		P

Clause	Requirement + Test	Remark	Verdict
5.5-2	(R) The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.		P
5.5-3	(R) Cryptographic algorithms and primitives should be updateable.		P
5.5-4	(RC) Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.		P
5.5-5	(MC) Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate.	The device doesn't support modifying the security settings of the device through the network interface.	N/A
5.5-6	(RC) Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.		P
5.5-7	(MC) The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.		P
5.5-8	(MC) The manufacturer shall follow secure management processes for critical security parameters that relate to the device.		P
5.6	Minimize exposed attack surfaces		/
5.6-1	(M) All unused network and logical interfaces shall be disabled.		P
5.6-2	(M) In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.		P
5.6-3	(R) Device hardware should not unnecessarily expose physical interfaces to attack.	.	P
5.6-4	(MC) Where a debug interface is physically accessible, it shall be disabled in software.	There are not accessible debug interfaces, so this test case is not applicable.	N/A
5.6-5	(R) The manufacturer should only enable software services that are used or required for the intended use or operation of the device.		P
5.6-6	(R) Code should be minimized to the functionality necessary for the service/device to operate.		P
5.6-7	(R) Software should run with least necessary privileges, taking account of both security and functionality.	The device is Embedded Operating System and doesn't support multi-user.	N/A

Clause	Requirement + Test	Remark	Verdict
5.6-8	(R) The device should include a hardware-level access control mechanism for memory.	All memory is controlled and managed by the RTOS running on the module (single process). therefore, it doesn't have to apply access control.	N/A
5.6-9	(R) The manufacturer should follow secure development processes for software deployed on the device.		P
5.7	Ensure software integrity		/
5.7-1	(R) The consumer IoT device should verify its software using secure boot mechanisms.	Local attacks are difficult because of restricted physical access.	N/A
5.7-2	(R) If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.	Local attacks are difficult because of restricted physical access.	N/A
5.8	Ensure that personal data is secure		/
5.8-1	(RC) The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.		P
5.8-2	(MC) The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.		P
5.8-3	(MC) All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.	The device doesn't have external sensing capabilities.	N/A
5.9	Make systems resilient to outages		/
5.9-1	(R) Resilience should be built into consumer IoT devices and services, considering the possibility of outages of data networks and power.		P
5.9-2	(R) Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.		P
5.9-3	(R) The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.	The load-balance capability is applied on cloud server as complementary measure. It's acceptable not to implement the order fashion on device.	N/A
5.10	Examine system telemetry data		/

Clause	Requirement + Test	Remark	Verdict
5.10-1	(RC) If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.	The device doesn't collect any telemetry data, so this test case is not Applicable.	N/A
5.11	Make it easy for users to delete user data		/
5.11-1	(MC) The user shall be provided with functionality such that user data can be erased from the device in a simple manner.		P
5.11-2	(RC) The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.	The device doesn't provide this functionality. But the personal data can be removed from associated services by unregistering you account on app.	N/A
5.11-3	(RC) Users should be given clear instructions on how to delete their personal data.		P
5.11-4	(RC) Users should be provided with clear confirmation that personal data has been deleted from services, devices and applications.		P
5.12	Make installation and maintenance of devices easy		P
5.12-1	(R) Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.		P
5.12-2	(R) The manufacturer should provide users with guidance on how to securely set up their device.	There's no security-relevant setting on the device.	N/A
5.12-3	(R) The manufacturer should provide users with guidance on how to check whether their device is securely set up.	There's no security-relevant setting on the device.	N/A
5.13	Validate input data		/
5.13-1	(MC) The consumer IoT device software shall validate data input via user interfaces or transferred via application programming interfaces (APIs) or between networks in services and devices.		P
6	Data protection provisions for consumer IoT		/
6-1	(MC) The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.		P
6-2	(MC) Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way.		P
6-3	(MC) Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.		P
6-4	(RC) If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality	The device doesn't support this ability to collect telemetry data.	N/A

Clause	Requirement + Test	Remark	Verdict
6-5	(MC) If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.	The device doesn't support this ability to collect telemetry data.	N/A

- - End of report - -

Appendix 1: Difference between models

No.	Product model	Main control board model	Main control board firmware version	Main control board PCB version
1	JE-3000A	HTE097-M-A3	HTE097M-A3_V1.28	25-0001-000005
2	JE-2000C	HTE097-M-A3	HTE097M-A3_V1.22	25-0001-000005
3	JE-1000B	HTE081-M-A4	HTE081M-A4_V2.0	07-2100-259061
4	JE-1000C	HTE103-M-A1	HTE103-M-A1_V2.0	25-0001-000009
5	JE-300B	HTE095-M-A3	HTE095-M-A3_V1.0	25-0001-000013

Details of: Outlook – Front view

Remark: Representative Model: JE-3000A



Details of: Outlook – Back view

Remark: Representative Model: JE-3000A



Details of: Outlook – Left side view

Remark: Representative Model: JE-3000A



Details of: Outlook – Right side view

Remark: Representative Model: JE-3000A



Details of: Outlook – Top view

Remark: Representative Model: JE-3000A

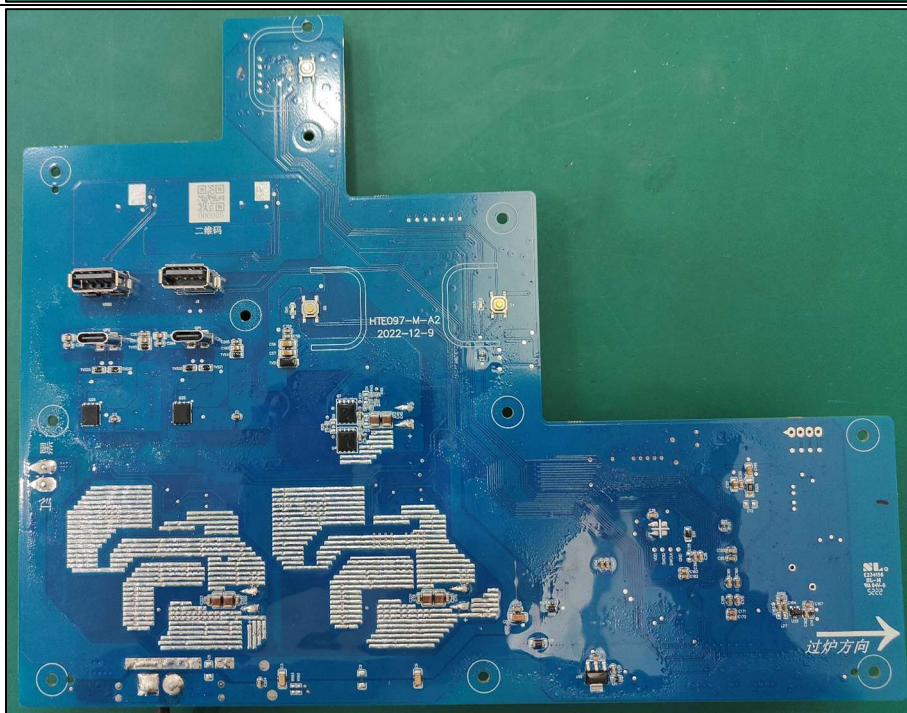
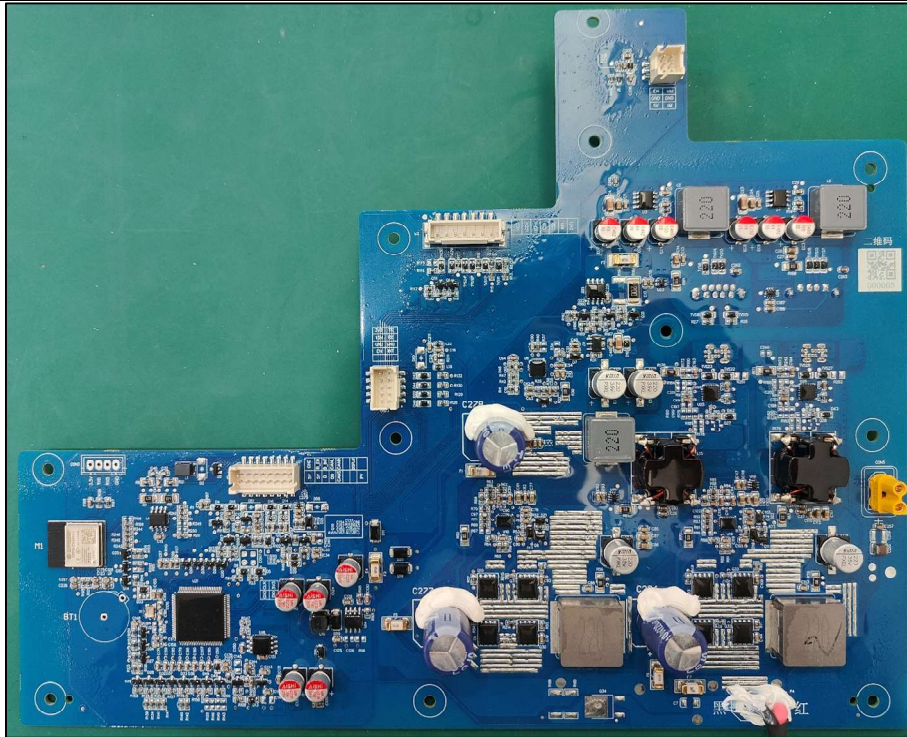


Details of: Outlook – Bottom view

Remark: Representative Model: JE-3000A



Details of: Device's main control board
Model: HTE097-M-A3
Remark: PCB version: 25-0001-000005



Details of: Wi-Fi Module

Remark: Model: ESP32-C3-MINI-1



Details of: Outlook
Remark: Model: JE-2000C



Details of: Outlook
Remark: Model: JE-1000B



Details of: Outlook
Remark: Model: JE-1000C

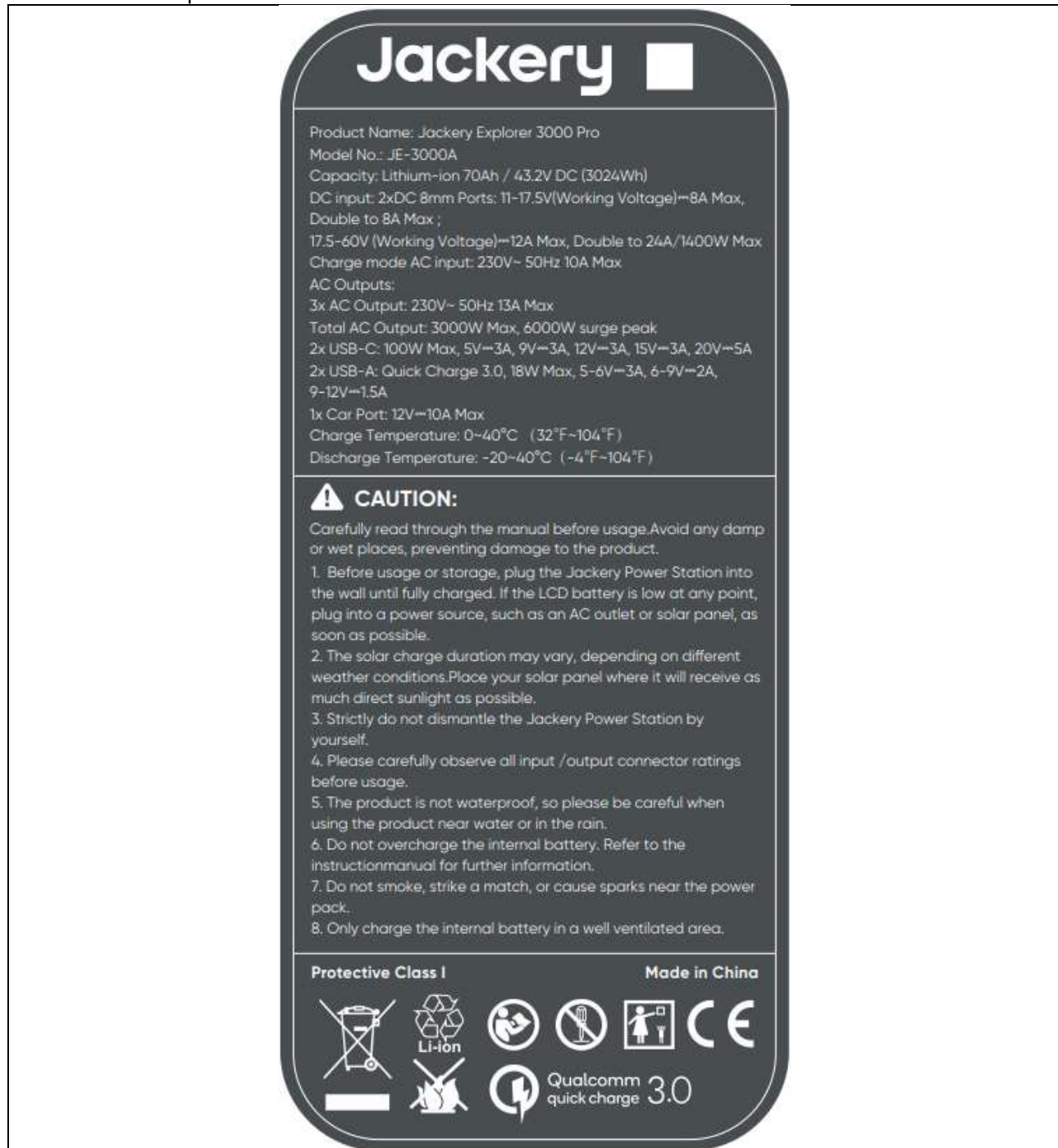


Details of: Outlook
Remark: Model: JE-300B



Details of: Label

Remark: Representative model: JE-3000A



Details of: Label
Remark: Model: JE-2000C



Details of: Label
 Remark: Model: JE-1000B

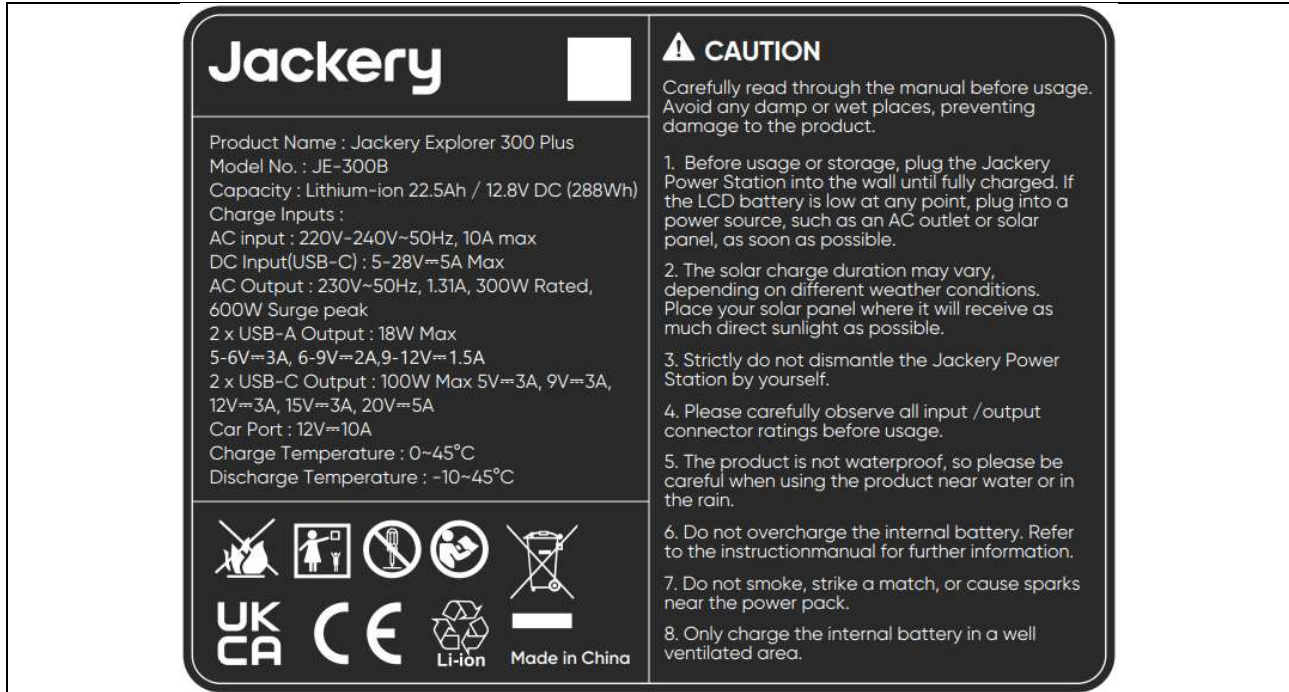
Jackery Product Name: Jackery Explorer 1000 Pro Model No.: JE-1000B Capacity: Lithium-ion 23.2Ah/43.2V DC(1002Wh) AC Input: 230V~ 50Hz, 10A Max DC Input: 12V-17.5V(Working Voltage)~8A, Double to 16A Max 17.5V-60V(Working Voltage)~11A, Double to 22A/800W Max 2 x AC Output: 230V~ 50Hz, 4.35A Max, 1000W rated output, 2000W peak surge 2 x USB-A output: Quick Charge 3.0, 18W Max 5-6V~3A, 6-9V~2A, 9-12V~1.5A 2 x USB-C Output: 100W Max 5V~3A, 9V~3A, 12V~3A, 15V~3A, 20V~5A Car Port: 12V~10A Charge Temperature: 0~40 °C Discharge Temperature: -10~40 °C		2. The solar charge duration may vary, depending on different weather conditions. Place your solar panel where it will receive as much direct sunlight as possible. 3. Strictly do not dismantle the Jackery Power Station by yourself. 4. Please carefully observe all input/output connector ratings before usage. 5. The product is not waterproof, so please be careful when using the product near water or in the rain. 6. Do not overcharge the internal battery. Refer to the instruction manual for further information. 7. Do not smoke, strike a match, or cause sparks near the power pack. 8. Only charge the internal battery in a well ventilated area.
⚠ CAUTION Carefully read through the manual before usage. Avoid any damp or wet places, preventing damage to the product. 1. Before usage or storage, plug the Jackery Power Station into the wall until fully charged. If the LCD battery is low at any point, plug into a power source, such as an AC outlet or solar panel, as soon as possible.	Qualcomm 3.0 quick charge CE Li-ion Made in China	

Details of: Label
 Remark: Model: JE-1000C

Jackery Product Name : Jackery Explorer 1000 Plus Model No. : JE-1000C Capacity : Lithium-ion 30.4Ah/41.6V DC (1264.64Wh) DC Input : Support 12~60V~11A Max, Double to 22A/800W Max AC Input : 220V-240V~50Hz, 10A Max 2x AC Output : 230V~50Hz, 8.7A, 2000W Rated, 4000W Surge peak 1x DC Expansion Port : 32.5V~46.8V~68A Max 2x USB-C Output : 100W Max, 5V~3A, 9V~3A, 12V~3A, 15V~3A, 20V~5A 2 x USB-A Output : 18W Max, 5-6V~3A, 6-9V~2A, 9-12V~1.5A Car Port : 12V~10A Charge Temperature : 0~45°C (32~113°F) Discharge Temperature : -10~45°C (14~113°F)		⚠ CAUTION: Carefully read through the manual before usage. Avoid any damp or wet places, preventing damage to the product. 1. Before usage or storage, plug the Jackery Power Station into the wall until fully charged. If the LCD battery is low at any point, plug into a power source, such as an AC outlet or solar panel, as soon as possible. 2. The solar charge duration may vary, depending on different weather conditions. Place your solar panel where it will receive as much direct sunlight as possible. 3. Strictly do not dismantle the Jackery Power Station by yourself. 4. Please carefully observe all input/output connector ratings before usage. 5. The product is not waterproof, so please be careful when using the product near water or in the rain. 6. Do not overcharge the internal battery. Refer to the instruction manual for further information. 7. Do not smoke, strike a match, or cause sparks near the power pack. 8. Only charge the internal battery in a well ventilated area.
UK CA CE Protective Class I Li-ion Made in China		

Details of: Label

Remark: Model: JE-300B



*** END OF REPORT ***