Product Vulnerability Management Plan

EN+ AC Charger

Date of Completion: 08-12-2022

Product vulnerability management plan is intended to create a robust process for addressing security issues reported in an EN+ product post-release, due to any third-party components used in the product, security weaknesses which might get introduced due to insecure coding practices and security issues reported by external entities e.g. independent security researchers, security organizations, governments, and customers etc. in the product (directly), when deployed in the field.

1. EN+ Source Inventory (Development Environment Security)

To manage and maintain a product and address any vulnerabilities in the future it is expected that the products follow the best practices in the industry for the following items

- Product Documentation
- Code Documentation Practices
- Use of Static/Dynamic Analysis tools
- NO Dead code in the product.
- Code refactoring at regular intervals
- Maintain an inventory of tools and environment (including the standard libraries & frameworks used) used to build and manage the release.

1.1. Product Documentation

Artifact	Available
System Requirements Specifications	YES
System Design Specifications	NO
System Architecture Diagram & Use Cases	YES
Software Development Plan	YES
Hardware Development Plan	NO
System Validation/Test Plan	YES
Cybersecurity Plan	NO

1.2. All EN+ source available under Source Control Management (SCM)?

☒ Yes ☐ No

1.3. Name of Tool used for Source Control Management (SCM)

Firmware：Tortoise SVN

APP and Cloud platform

These tools maintained by special personnel in EN+ to ensure that this tool can be upgraded in a timely manner according to the publisher's update suggestion.

Tortoise SVN

1.4. Name of Code Documentation Tool used

Firmware：Visual Studio Code

APP and Cloud platform ： Android studio, Xcode, Visual Studio Code, HBuilder,

These tools maintained by special personnel in EN+ to ensure that this tool can be upgraded in a timely manner according to the publisher's update suggestion.

1.5. Build Environment

Build Host OS and Version:

Charger OS:We use RTOS system in ST(ucOS) chip and ESP32(FreeRTOS)

Toolchain Used and Version

Windows:

Keil MDK Version 5 Community version

IntelliJ IDEA

Android studio

Ubuntu 20.04: esp32-IDF

Mac OS:Xcode

1.6. Code Static Analysis tools used

☐ Coverity ☐ Polyspace

☐ Others (findbugs,Checkstyle) ☒ None

1.7. Scanning for Software Weaknesses (CWEs)

Define a process to scan the source code for software/firmware using a Source Code Analysis Tool (SAST) preferably Coverity, using the guidelines provided here. The process should address, at a minimum, the below points,

- The process should define timelines to address the CWEs identified during the scan.
- Triage the CWEs as per the guidelines provided in the guidance document.
- **Latest version of Coverity Analysis tool shall be used, unless otherwise approved by R&D**
- If the SAST tools is different from Coverity, provide a report on how the tool is covering the CWEs specified in the guidance document.

2. Software Bill of Material

- Product team shall create a Software Bill of Material for all the Third-Party components used in the software/firmware development for the product, for all the production releases, with below information –
- Component name
- Component Version
- Vendor of the component
- Used in Firmware/Software
- Link to the vendor site or product

NOTE: The Software Bill of Material should contain both open source and commercial third party libraries used in the product.

2.1. Have you created a Software Bill of Material?

☒ Yes ☐ No ☐ Not Applicable

2.2. Have you shared the Software Bill of Material with R&D?

☒ Yes ☐ No ☐ Not Applicable

If the answer to above questions is No or Not Applicable, provide a proper rational for the same.

3. Hardware Bill of Material

All the hardware components used in the product should be documented with below information –

SoC Vendor Name (E.g., ADI)

SoC Family Name (E.g., Blackfin)

SoC Part Number (E.g., GD32F303VCT6)

SoC Firmware Name & Version (E.g., vybrid_mvf30ns151cku26_firmware)

SoC Toolchain used

3.1. Have you created a Hardware Bill of Material?

☒ Yes ☐ No ☐ Not Applicable

3.2. Have you shared the Hardware Bill of Material with R&D?

☒ Yes ☐ No ☐ Not Applicable

4. Scanning for CVEs in Third party components

Define a process to scan the binaries or integrate the scanning capability in the CI/CD pipeline (Software/Firmware) to identify CVEs in the Third-Party Components used in the product development as per EN+'s Product Cybersecurity Third-Party Components Risk Management Policy.

The process should, at a minimum, have the below points

- Risk assess the CVEs and prioritize to address Critical/High CVEs
- Triage the CVEs identified in the Components during scanning tools like Black hub, BDBA, CVE Manager etc.
- Timelines to update the Third-party components (Monthly, Quarterly, Half Yearly, Release Cycle)

5. Monitoring for End-of-Life Components (Third party components)

Define a process to monitor the Third-Party components for End of life as per EN+'s Product Cybersecurity for Third-Party Components used in the software/firmware. Process should include, at a minimum, to address the below points – Obtain a support plan from Third-Party component vendors, if provided.

- Plan to replace the EOL components as per support plan provided by OEM vendors.
- Obtaining the EOL timelines for all the Third-Party Components.
- Obtaining End of support from SoC Vendors (Hardware).

1. According to the component supplier's notification, for components that need to be replaced, the replacement process will be introduced after internal evaluation. This process includes the evaluation and testing of alternative components, and small batch trials. After the process is completed, the ECR process is initiated for all related products to switch components., the original components are not in use after the switch;

2. Hold software network security meetings with SOC suppliers on a quarterly basis, and evaluate whether to perform component switching and scrapping according to their recommendations;

3. The used components will be counted every quarter. If any components have not been used for more than 1 year, a scrapping process will be initiated to assess whether they need to be scrapped.

4.7 days for initial response are defined according to the published vulnerability disclosure policy. By no later than 60 days after receiving the vulnerability a fix will be released or a warning is published, as it is assured by contract with the third parties.

6. Supplier Contract with Vendors

Product team should have a supplier contract with vendors for off-the-shelf commercial component providers that outlines:

- A process to receive notifications (within a specified time limit, for example, 5 days, points (person) of contact) of a vulnerability discovered in their library.
- A process to receive updates fixing the discovered vulnerability.
- The contract should include agreed upon timing of when a patch should be available and a methodology for coming into agreement on the severity of a vulnerability (roles and responsibilities)
- A process to receive normal ongoing updates in the library with appropriate documentations.

6.1. Do you have the contract signed with software vendors with above cybersecurity recommendations?

☐ Yes ☒ No ☐ Not Applicable

6.2. Do you have the contract signed with hardware vendors with above cybersecurity recommendations?

☐ Yes ☒ No ☐ Not Applicable

7. Externally Reported Vulnerabilities

Define a process to receive and address the externally reported vulnerabilities in the products when the products are deployed in production. The process should be aligned with EN+'s vulnerability disclosure policy. The process should, at a minimum, address the below point.

1. The network security problems found in the operation of the product will be directly fed back to SPOC via email support@en-plus.com.cn;

2. SPOC should organize the R&D team to analyze the problem immediately after receiving the problem, and provide the problem analysis report and solution plan within 72 hours;

3. Before the completion of the network security incident close, SPOC will notify the relevant responsible persons of the work progress every week, and the responsible persons of all relevant persons will review the "Event Review Report" to mark the completion of the handling of the incident.

4. After the Software Testing Department tests the new software without any problems, a test report needs to be issued, and the R&D decides whether to upgrade according to the test report. If an upgrade is required, the R&D team will provide a version upgrade plan proposal to the Customer Service. After approval by the Customer Service, the two teams will jointly complete the software upgrade of the running terminal and the hardware in production;

5. After the upgrade event is completed, the R&D team will lead a complete review of the event and output the "Event Review Report" (including the retrospective of the cause of the problem, the treatment plan and the follow-up improvement measures);

6. Before the completion of the network security incident close, R&D will notify the relevant responsible persons of the work progress every day, and the responsible persons of all relevant persons will review the "Event Review Report" to mark the completion of the handling of the incident;

7.7 days for initial response are defined according to the published vulnerability disclosure policy. Usually 90 days after receiving the vulnerability a fix will be released or a warning is published. The warning will be withdrawn since a fix is released.

8. Customer Communications

In the event of externally or internally identified vulnerabilities, an EN+ based product webpage should be used to post customer notifications of vulnerabilities and pending new releases that address cybersecurity vulnerabilities.

9. Response Processing Time

Service Level	Level Name	Level Definition	SLA	Emergency response time	System recoverty time
L0	Core services	In case of any exception, it will affect all main business	20 minutes	7days	30days
L1	key services	Once exceptions occur, it will affect some branch business	20 minutes	10days	30days
L2	General services	Once the exception occurs, the main business process will not be affected.	20 minutes	15days	60days
L3	Peripheral services	Once the exception occurs, it is imperceptible to users.	20 minutes	30days	90days

10. Report an Issue

If you believe you have found a security vulnerability in a currently supported EN+ product, you can choose to report this vulnerability to EN+, you acknowledge that you have read and accepted EN+'s Vulnerability Disclosure Policy.

Contact -

support@en-plus.com.cn

Definitions

Third party components – All open-source components and commercial components which are obtained from a 3rd party vendor or open-source market are considered as Third-party components.

- Open-source components – E.g., Linux Kernel, zlib, openssl, openssh,
- Commercial Components – E.g., DNP3 Library, Modbus Library,

Revision History (Product Teams can delete this section in the final document)

Version	Date	Comments
A	Feb 2018	Created initial process document
B	June 2018	Update to include the Supplier contract for Third Party Components
C	June 2022	Added Section 8 to address customer communications Added Section 9 to “Report an Issue”