Espressif Security Incident Response Process

Version 1.0
Espressif Systems
Copyright © 2023

Table of Contents

1. Introduction

Espressif is committed to ensuring the security of its products and software solutions. We recognize that security incidents are a constant threat, and we place a high priority on responding to and mitigating them in a timely and effective manner.

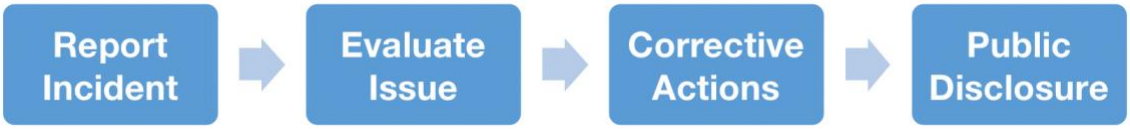
This document highlights the process for dealing with security incidents that may arise in Espressif hardware products and software solutions. This policy will be regularly reviewed and updated to ensure that it remains effective and aligned with the industry best practices.

2. Process Workflow

Process starts when an issue is discovered, for example, from third party project disclosure, researcher, or vulnerability report including Espressif Bug Bounty Program (BBP), customer report and internal discovery.

Process ends when all applicable fixes have been merged, and a public security disclosure has been published, if applicable. Public security disclosure will be published in Espressif website > Page Advisories > Category **Security**, which contains both hardware and software disclosures. ESP-IDF software components specific advisories are published in ESP-IDF GitHub Repo > Tab Security.

Process Workflow:



2.1. Report Incident

There are several ways an incident may be reported, internal discovery by Espressif employees, external reported by customer, researcher or other interested parties. Reporter can submit the security vulnerability through:

- Hardware Issues Form, Software Bug Form
- Espressif Bug Bounty Program (Security issues in Espressif software solutions reported at bugbounty@espressif.com can qualify for our Bug Bounty Program)

Note: In consideration of the sensitivity of the information being shared, Espressif strongly advises that all security vulnerability reports should be submitted in an encrypted format, using the Espressif PGP/GPG key.

- Fingerprint: A855 92F9 A412 44C1 13F9 0F0F 01C3 E225 A0FE D438
- Public Key File (ZIP, 4 KB)

Please access the following free software to read and author PGP/GPG encrypted messages:

- Gpg4win
- GnuPG

When you report potential discovered security vulnerability, please provide as much necessary information as possible to help us rightly assess the reported security vulnerability, including but not limited to:

- Clear and concise issue title, specifying the impacted Espressif products by including the product name or part number.
- Issue description, including software version, hardware revision used during testing, tools employed and other environmental factors, your expected test result and actual test result, and security impact of the issue.

- Complete steps to reproduce the issue, detailed test codes that can be run after compilation and debug logs. Additionally, include any additional information that may be relevant.

In the absence of sufficient information, the evaluation process may take longer.

2.2. Evaluate Issue

- Internally review if all necessary information is provided, assign priority, and create tracker.
- Conduct technical analysis of the issue, determine its validation and impact on Espressif products. Assess security risk and categorize the issue.
- Time estimate – 4 weeks

2.3. Corrective Actions

- Produce fix or mitigation actions if the potential vulnerability is verified.
- Communicate the response to the report submitter and others where appropriate.
  - Timeline and version(s) for any fixes. Ask the issue reporter to verify the patch (if applicable).
  - Timeline estimated to publish advisory (if any).
  - Analyze the need to register CVE for the issue.
  - Determine eligibility and reward level for BBP (if applicable).
- Deploy the fix and mitigation actions.
- Prepare and review the security incident advisory and reserve CVE number (if applicable).
- Time estimate – 8 weeks (about 2 months) from start

2.4. Public Disclosure

On agreed disclosure date:

- Publish the public advisory document, including any findings, impacts, remediation activities or security enhancements plan for our product roadmap. Mark any CVE identifier as visible.
- Ensure the remaining fixes are rapidly deployed to the software stack e.g., ESP-IDF.
- In the case of BBP, pay a reasonable bounty.
- Notify affected Espressif customers, if necessary.
- Time estimate – 12 weeks (about 3 months) from start

Note: The time estimates specified above are typical timelines, and actual timelines may vary depending on the severity and complexity of the issue.

3. Disclosure Policy

Espressif values the contributions made by security researchers and the significant role they play in enhancing the security of our products. To ensure the effectiveness of the security incident response, we suggest that incident reporters follow the coordinated vulnerability disclosure process, which involves reporting vulnerabilities to us and allowing time for investigation and remediation before disclosing any information publicly. Additionally, we also recommend that incident reporters do not disclose any unresolved or unpublished vulnerabilities without prior authorization from Espressif.

During the coordinated vulnerability disclosure process, Espressif maintains strict confidentiality of sensitive information. Any information shared between Espressif and the incident reporter will be kept confidential and only used for the purpose of addressing the reported vulnerability.

Espressif would like to express its gratitude to everyone who contributes to keeping our products and users safe.

www.espressif.com

Disclaimer and Copyright Notice

Information in this document, including URL references, is subject to change without notice.

ALL THIRD PARTY'S INFORMATION IN THIS DOCUMENT IS PROVIDED AS IS WITH NO WARRANTIES TO ITS AUTHENTICITY AND ACCURACY.

NO WARRANTY IS PROVIDED TO THIS DOCUMENT FOR ITS MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, NOR DOES ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

All liability, including liability for infringement of any proprietary rights, relating to use of information in this document is disclaimed. No licenses express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

The Wi-Fi Alliance Member logo is a trademark of the Wi-Fi Alliance. The Bluetooth logo is a registered trademark of Bluetooth SIG.

All trade names, trademarks and registered trademarks mentioned in this document are property of their respective owners, and are hereby acknowledged.

Copyright © 2024 Espressif Systems (Shanghai) Co., Ltd. All rights reserved.