Espressif Security Vulnerability Report Form

Bug Bounty Program Submission Template | v1.1

How to Submit

Send this completed form to: **bugbounty@espressif.com**

PGP/GPG Encryption (strongly recommended):

Fingerprint: **A855 92F9 A412 44C1 13F9 0F0F 01C3 E225 A0FE D438**

Public key and instructions available in the Espressif Security Incident Response Process document.

Program Overview

Reward: Bug bounty rewards typically range from USD $200 to $3,600 depending on severity and impact. Final reward amounts are at Espressif's sole discretion.

Acknowledgment: Espressif aims to acknowledge receipt within 7 business days and provide a tracking reference ID for your submission.

Timeline: Per the ESIRP: Evaluation ~4 weeks, Corrective Actions ~8 weeks, Public Disclosure ~12 weeks from report. Actual timelines may vary depending on severity and complexity.

Disclosure: Espressif follows a coordinated vulnerability disclosure process (~90 days). Reporters agree not to disclose publicly before Espressif releases advisories and/or fixes.

Safe Harbor: Espressif will not pursue legal action against security researchers who report vulnerabilities in good faith, comply with this program's terms, and follow the coordinated disclosure process.

Out of Scope: Vulnerabilities in third-party libraries, third-party services not operated by Espressif, example-only code (unless the same pattern exists in production SDK), and issues in software outside the longevity commitment period.

Section 1 — Reporter Information

Reporter Details	
Name / Alias	Your name or handle
Email Address	Contact email for correspondence
Organization (if any)	Company or research group, or Independent

Date of Submission	YYYY-MM-DD
Espressif Reference ID (if any)	Tracking ID from prior communication, if applicable

Section 2 — Vulnerability Overview

Issue Summary	
Vulnerability Title	Short descriptive name, e.g., " Heap overflow in BLE GATT handler "
Affected Product(s)	e.g., ESP32-S3, ESP32-C3 Specify SoC, module, or dev board
Affected Software	SDK/Framework: e.g., ESP-IDF v5.3.1 Managed Component: e.g., esp_tls v1.2.0 Cloud/App: e.g., ESP RainMaker SDK v1.0
Version Tested	Exact version/commit hash used in your PoC
Affected Version Range (if known)	e.g., v5.1.0 through v5.3.1; is the latest release affected?
Branch / Release Status	☐ Official release version ☐ Development / master branch ☐ Component not yet on Component Manager ☐ Other (please specify)
Affected Component / Module	e.g., Bluetooth stack, Wi-Fi driver, flash encryption, secure boot
Bug Description	Provide a clear, detailed description of the vulnerability. What is the root cause? What boundary or assumption is violated? What is the security consequence?
Related CVE(s) (if any)	e.g., CVE-2024-XXXXX, or " None known ". Helps identify duplicates and regressions.

Section 3 — Environment and Reproduction

3.1 Proof-of-Concept Environment

Indicate the environment used for your PoC. Reports validated on real hardware receive higher consideration.

PoC Environment	
Environment Type	☐ Actual hardware setup *(strongly recommended)* ☐ Emulator or host OS environment ☐ Other (please specify below)
If other, please specify	Describe the environment
Hardware Setup Details	Board/module model, revision Any external peripherals or connections

3.2 Device Security Configuration

Indicate which security features were enabled during testing. Issues demonstrated under Espressif's recommended security configuration receive higher consideration.

Security Configuration	
Active Security Features	☐ Secure Boot enabled ☐ Flash Encryption enabled ☐ Production firmware / Release mode ☐ Default recommended security configuration ☐ Other (please specify below)
Configuration Details	Any non-default settings, custom partitions, debug flags, etc.

3.3 Reproduction Steps

Provide complete steps to reproduce the issue. This is the most critical part of your report.

Reproduction Details

Step-by-step reproduction procedure:

1. ...
2. ...
3. ...

Test code:

Attach or paste compilable code that demonstrates the issue

Test code 1

Test code 2

Test code 3

Log output / crash evidence:

Paste relevant logs, stack traces, core dumps, or screenshots

Log output 1

Log output 2

Log output 3

Section 4 — Attack Assessment

4.1 Attack Preconditions

Preconditions	
Physical access required?	☐ Remote (internet / external network) ☐ Local / Adjacent (shared network, BLE/Wi-Fi range) ☐ Physical (requires hands-on device access)
Special equipment required?	e.g., JTAG debugger, oscilloscope, EM probe, fault injection glitcher Estimated cost of equipment if applicable
Privileges or access required?	e.g., authenticated user, physical UART, Wi-Fi proximity, none
Additional conditions	Any other prerequisites for the attack to succeed

4.2 Impact Assessment

Select the capability the attacker gains. This helps Espressif assess severity and determine the appropriate response.

Impact	
Primary Impact	☐ Service disruption (e.g., DoS, crash) ☐ Information disclosure (e.g., reading sensitive memory) ☐ Unauthorized access (e.g., via authentication bypass) ☐ Privilege escalation (e.g., gaining elevated permissions) ☐ Access to protected data/functions (e.g., crypto/security bypass) ☐ Arbitrary code execution (e.g., RCE) ☐ Supply chain compromise (e.g., build pipeline, component registry, code signing) ☐ Other (please specify below)
Impact Description	Describe the real-world consequence of this vulnerability. Does it affect confidentiality, integrity, or availability? Is the impact scalable across multiple devices? Does it affect root of trust or long-lived keys?
Affected Trust Boundary	☐ Application layer only ☐ Platform / system level ☐ Root of trust

4.3 CVSS Score (Optional)

If you are familiar with CVSS, providing a self-assessed score helps speed up triage. This is optional and Espressif will perform its own assessment.

CVSS Self-Assessment

CVSS Version	☐ CVSS v3.1 ☐ CVSS v4.0 ☐ Not provided
CVSS Vector String	e.g., CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS Base Score	e.g., 9.8 Critical

Section 5 — Suggested Mitigation

Known Mitigations or Workarounds
If you are aware of any workaround, configuration change, or mitigation that reduces the impact of this vulnerability, please describe it here. This helps Espressif provide interim guidance to customers while a full fix is developed.

Section 6 — CVE and Disclosure

CVE and Disclosure Preferences	
CVE Suggestion	Do you suggest Espressif register a CVE for this issue? ☐ Yes ☐ No ☐ Not sure
Credit Preference	If a CVE is registered, would you like to be credited? ☐ Yes, credit me as - "please specify name and/or company" ☐ No, keep me anonymous
Planned Disclosure	Do you plan to publicly disclose this vulnerability? ☐ Yes (will coordinate with Espressif per ~90-day policy) ☐ No

Section 7 — Additional Context and Attachments

Additional Details
References and related research:
Links to related advisories, papers, blog posts, or prior CVEs
References 1
References 2

References 3

Attachments:

List any attached files: PoC code, scripts, pcap captures, photos of hardware setup, etc.

Attachments 1

Attachments 2

Attachments 3

Any other information:

Anything else that would help Espressif reproduce and resolve the issue

Other info 1

Other info 2

Other info 3

Section 8 — Submission Agreement

Terms and Acknowledgment

By submitting this report, I confirm that:

☐ I have read and agree to the Espressif Bug Bounty Program terms and conditions as outlined in this form and the Espressif Product Security Incident Response Process.

☐ I understand that bounty rewards are at Espressif's sole discretion and are determined based on severity, report quality, and reproducibility.

☐ I understand that if I fail to provide requested information within a reasonable timeframe, Espressif may terminate the evaluation process for this submission.

☐ I agree to follow the coordinated disclosure process and will not publicly disclose this vulnerability before Espressif releases advisories and/or fixes.

☐ I agree not to independently register a CVE for this issue before notifying Espressif.

☐ The information provided in this report is accurate to the best of my knowledge.

Name (typed or signed):

Date:

Reference: Expected Processing Timeline

Based on the Espressif Security Incident Response Process (ESIRP v1.0). Actual timelines may vary depending on severity and complexity.

Stage	Timeline	Activities
1. Report Incident	Day 0	Submit via bugbounty@espressif.com. Acknowledgment with tracking reference ID within ~7 business days.
2. Evaluate Issue	~4 weeks	Internal review, priority assignment, tracker creation. Technical analysis, validation, impact assessment, and risk categorization.
3. Corrective Actions	~8 weeks from start	Produce fix or mitigation. Communicate response to reporter. Determine fix timeline, CVE need, and bounty reward eligibility. Deploy fix and prepare advisory.
4. Public Disclosure	~12 weeks from start	Publish advisory. Mark CVE as visible. Deploy remaining fixes. Process bounty payment (if applicable). Notify affected customers if necessary.

Note: Bounty reward determination happens during Corrective Actions. Final reward amounts are at Espressif's sole discretion.

For the full process, including reporting channels, evaluation criteria, and disclosure timelines, please refer to the **Espressif Product Security Incident Response Process**.

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.