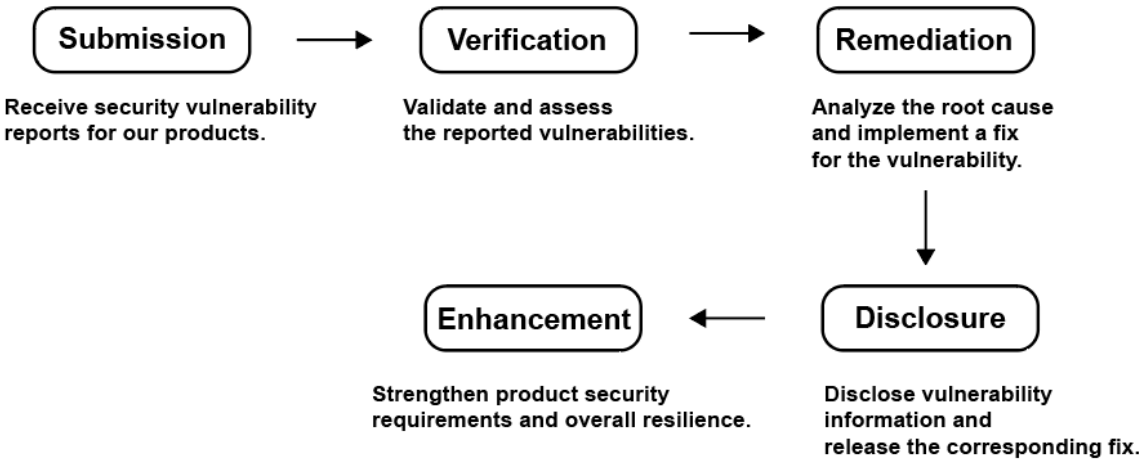
Yealink Vulnerability Disclosure Policy

Introduction

Yealink welcomes feedback from security researchers and the public to help us enhance our security measures. We would like to hear your feedback if you find any potential security vulnerabilities in any of our assets. This policy outlines the steps for reporting vulnerabilities, our expectations, and our response process.

Vulnerability Response Process



Scope

Guidelines

- If you discover a potential security vulnerability, please notify us immediately. Do not attempt to verify vulnerabilities yourself.
- Only use or access accounts and information that belong to you.
- Please do not damage or modify data that does not belong to you.
- Please do not degrade the performance of Yealink products and services or the performance of user products and services.
- Do not perform social engineering, physical or denial of service attacks against Yealink personnel, locations or assets.
- Comply with this vulnerability disclosure policy and all applicable laws.

Within the Scope

- This policy applies to Yealink's products, services, and systems. Please carefully confirm the ownership of the assets you are testing during your research.
- If you discover vulnerabilities in vendor systems that are beyond the scope of this policy, please report them directly to the vendor through their disclosure program.
- If you are unsure whether a certain system is within the scope or need assistance reporting discovered content to the vendor, please get in touch with us at security@yealink.com. We are happy to assist!

Out of Scope

- Assets or other equipment owned by parties not involved in this policy.
- The attack requires MITM or physical access to user devices.
- Device configuration error that does not comply with best practices.
- The vulnerability is caused by outdated software or unsupported products.
- Affected users use outdated browsers that are lower than two stable versions below the latest released stable version.
- Social engineering attacks such as phishing are required.

Safe Harbor

When conducting vulnerability research with the aim to contribute to overall internet security, we will regard your work as useful and performed in good faith. Hence:

- We will not take legal action against you for any unintentional or good-faith violations of this policy, provided that you comply with applicable anti-hacking laws and regulations.
- We will not make any claims against you for bypassing technical controls, provided that you comply with relevant anti-circumvention laws and regulations.
- We waive these restrictions to a limited extent that may interfere with security research in our Terms of Service (TOS) and/or Acceptable Use Policy (AUP).

You still need to comply with all applicable laws. If a third party initiates legal action against you and you have complied with this policy, we will take measures to provide

evidence demonstrating that your actions were conducted in compliance with this policy.

If you have any doubts or are unsure if your security research complies with this policy, please submit a report through our official channels before proceeding further.

Please note that the safe harbor only applies to legal claims under the control of organizations participating in this policy, and this policy does not bind independent third parties.

Vulnerability Report

For Yealink customers and partners, they can report security issues and provide all relevant information through the technical support ticket system (https://ticket.yealink.com/). Non-Yealink customers or partners can send an email to security@yealink.com for security researchers. The more detailed information you provide, the easier for us to solve the problem.

Yealink promises to respond to the report as soon as possible and keep you informed of our progress throughout our investigation and/or mitigation of the security issue you reported. Within one business day after your initial contact, you will receive a non-automated email or ticket reply confirming that we have received the reported vulnerability. And you will receive updates on the processing progress from us within five working days.

Our Expectations of You

To help us identify potential vulnerabilities and facilitate the remediation process, an excellent vulnerability report should include the following:

- Describe the vulnerability, the exact location where it was found, and the real-world impact.
- Detailed description of the steps required to reproduce the vulnerability (POC, screenshots and videos would be helpful).
- Each report only includes one vulnerability (unless it belongs to an attack chain).
- When there is no evidence of malicious exploitation, please do not report the results of the automatic scanner

What You Can Expect From Us

When you choose to share contact information with us, we promise to coordinate with you as openly and quickly as possible:

- We will confirm receipt of your report within one business day.
- We will evaluate your submitted report, notify you of the validity and the corresponding remediation plan, and express our sincere appreciation for your contribution.
- We use the Common Vulnerability Scoring System (CVSS) v3.1 to assess the severity of vulnerabilities in our products.
- We will do our best to confirm whether the vulnerability you reported exists, and strive to ensure the openness and transparency of the repair process, including the possible problems and challenges that may cause the vulnerability to be resolved in a timely manner.
- Upon confirmation of a vulnerability, detailed information and the corresponding remediation plan will be published on our Security Advisory page following the completion of vulnerability analysis and the implementation of the fix.
- We will insist on discussing issues through open dialogue.

Intellectual Property

Participating in Yealink vulnerability reporting program will not grant you or any third party any rights to Yealink intellectual property, products, or services. All rights not expressly granted in this policy are reserved by Yealink.

By submitting your report, you hereby consent that Yealink may use your findings to remedy any security in Yealink products.