Responsible Disclosure Policy

Introduction

At **the Mylaps group**, we are committed to maintaining a secure environment for our users. We appreciate the efforts of security researchers and community members who help us identify vulnerabilities. This Responsible Disclosure Policy outlines how you can report security issues related to our products and services. We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it.

We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

Scope

This policy applies to all consumer and B2B Internet of Things (IoT) devices developed, manufactured, or distributed by **the Mylaps group,** as well as our infrastructure. The devices include those connected to network infrastructure (such as the Internet or home/company network) and their interactions with associated services.

Reporting Vulnerabilities

If you discover a security vulnerability in any of our products or services, please follow these steps:

1. **Report the Issue**: Send an email to our security team at security@mylaps.com with detailed information about the vulnerability. Include the following:

- *Asset* (web address, IP Address, product or service name) where the vulnerability can be observed
- *Title of vulnerability* (mandatory)
- *Weakness* (e.g. CWE) (optional)
- *Severity* (e.g. CVSS v3.0) (optional)
- *Description of vulnerability* (this should include a summary, steps to reproduce, supporting files/relevant logs/screenshots and possible mitigations or recommendations) (mandatory)
- *Impact* (what could an attacker do?) (mandatory)

2. **Triage and Assessment**: Our security team will promptly review your report. We appreciate your patience during this process.

3. **Fix and Disclosure**: Once we verify the vulnerability, we will work on a fix. We commit to providing timely updates on the progress.
4. **Acknowledgment**: We value your contribution to our security. If you wish, we will acknowledge your efforts in our security advisories or release notes. Alternatively, you can remain anonymous.

Guidelines for Responsible Disclosure

To ensure a smooth process, please adhere to the following guidelines:

After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 10 working days. We will also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Once your vulnerability has been resolved, we welcome requests to disclose your report. We would like to unify guidance to affected users, so please do continue to coordinate public release with us.

Do NOT:

• Break any applicable law or regulations

• Access unnecessary, excessive or significant amounts of data

• Modify data in **The Mylaps Group**'s systems or services

• Use high-intensity invasive or destructive scanning tools to find vulnerabilities

• Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests

• Disrupt the **The Mylaps Group**'s services or systems

Disclaimer

While we strive to address security issues promptly, we cannot guarantee immediate fixes. By participating in responsible disclosure, you agree to follow the guidelines outlined here.

Thank you for helping us improve the security of our products and services!