Whereby

Vulnerability Disclosure Policy

Introduction

We in Whereby are committed to strengthen the security of our platform and services thus welcoming security researchers to disclose any vulnerabilities found directly to us.

This policy describes how Whereby works with the security community in the context of finding and responsibly reporting security vulnerabilities.

Reading this policy prior to reporting any security vulnerability is mandatory as it clearly describes what is not allowed, what is allowed and how these vulnerabilities can be reported responsibly. Failing to follow this policy will reduce the chance of a response to your vulnerability report and the chance of an honorable mention or bounty, in case it is applicable.

Last document update: July 1st, 2021

Security researchers must not:

- Disrupt Whereby systems or services.
- Modify or destroy data of Whereby systems or services.
- Disclose any found vulnerabilities to the public or third parties.
- Violate the privacy of Whereby users, employees, systems or services.
- Use high-intensity invasive, automatic or destructive scanning / exploit tools.
- Require financial compensation under threat of withholding or release of vulnerabilities to the public.
- Use malware.
- Use the discovered vulnerability in any way beyond proving / demonstrating its existence (e.g., exploit the vulnerability to pivot to internal systems, compromise a system and persistently maintaining access to it, etc).
- Use social engineering, spam or phishing techniques.

In order to protect our customers and services, we ask security researchers to securely delete any data retrieved during research as soon as the data is no longer required or within a month of the vulnerability being resolved, whichever occurs first.

Reporting

If you believe you've discovered a security vulnerability in one of our services, please email us at security@whereby.com

A vulnerability report should contain:

- Detailed description of the discovered vulnerability and its potential impact
- Date and time when the vulnerability was discovered
- Detailed description of the steps required to recreate the vulnerability

We will:

- Confirm the receipt of the report within 10 working days
- Investigate and verify the presence of the vulnerability
- Address the vulnerability and develop a fix
- Notify you when the vulnerability has been fixed

Please allow a reasonable time to address the discovered vulnerability. Fixes and mitigations are prioritized depending on the impact severity and ease of exploitation. We will make our best effort to communicate every update throughout the entire process. Researchers are welcomed to inquire about updates within reason (please no more than once every 14 days).

If you do find critical information, such as Personal Identifiable Information or financial information, please include the urgency of the matter in the subject line of your email to the Whereby security team.

Out-of-Scope Vulnerabilities

- TLS/SSL configuration weaknesses (e.g., weak / insecure cipher suites, renegotiation attacks).
- Vulnerabilities obtained via the compromise of a Whereby customer or Whereby employee accounts.
- Denial of Service (DoS / DDoS) attacks against Whereby systems or services.
- User interface bugs or typos.
- Login / logout CSRF.
- Missing HTTP security headers that do not lead directly to a vulnerability.
- Presence / absence of DNS records.
- Password, email and account policies (e.g: email id verification, password complexity).

- Attacks requiring physical access to a user's device.
- Report the use of a known-vulnerable library (without evidence of exploitability).
- Missing cookie flags without clearly identified security impact.
- Open redirectors.
- CSRF or clickjacking with no practical use to attackers
- CSRF that requires the knowledge of a secret.
- Exposed metrics or other type of not confidential data.
- Missing best practices, configuration or policy suggestions.
- Vulnerabilities that require a man-in-the-middle scenario to be exploited.

Previously reported vulnerabilities or security vulnerabilities already discovered by internal procedures are not eligible.

Recognition

Vulnerabilities reported and acknowledged to be valid are subject to public recognition of the author on our upcoming Hall of Fame page, depending on the criticality of the vulnerability. Any form of compensation will be considered but will not be guaranteed. This is dependent on the criticality of the vulnerability and the then-current budget.

In addition, security researchers that are able to submit a valuable security vulnerability will be added to our private Bug Bounty Program in the future.

Safe Harbor

Whereby will not take legal action against security researchers who submit vulnerability reports following the terms indicated in this document or for accidental, good faith violations of this policy, as long as the reason for the accidental / good faith violation has been clearly stated.

Whereby

Whereby reserves the right to modify the terms and conditions of this policy. By reporting a security vulnerability to Whereby on or after that effective date, you agree to the then-current Terms.

Whereby

Cookie Policy

Privacy Policy

GDPR Statement

VDP

Sitemap