Navigil Service

Vulnerability Disclosure Policy

v. 1.0

22/12/2022

Vulnerability Disclosure Policy

Navigil Ltd

Navigil Ltd is a caring company that provides industry benchmark services and wearable wellness products used by active elderly but also older adults needing support. Wearable product users are supported by family and friends as well as professional care providers.

We have developed this policy to both reflect our corporate values and to uphold our legal responsibility to good-faith security researchers that are providing us with their expertise.

Initial Scope

Navigil's Vulnerability Disclosure Program initially covers the following products:

- Navigil Service - web
- Share & Care - app
- Rafael - web
- S1/S3 watches
- 580 watches
- Navigil web pages – www.navigil.com

We ask that all security vulnerability reports are submitted only for the product stated in the above list.

Researchers who submit a vulnerability report to us will be given full credit on our website once the submission has been accepted and validated by our product security team.

Legal Posture

Navigil ltd will not engage in legal action against individuals who submit vulnerability reports to our security email. We openly accept reports for the currently listed Navigil Ltd products. We agree not to pursue legal action against individuals who:

- Engage in testing of systems/research without harming Navigil Ltd or its customers.
- Engage in vulnerability testing within the scope of our vulnerability disclosure program and avoid testing against [prod.navigil.io, ustest.navigil.io, usprod.navigil.io].
- Test on products without affecting customers, or receive permission/consent from customers before engaging in vulnerability testing against their devices/software, etc.
- Adhere to the laws of their location and the locations of Navigil. For example, violating laws that would only result in a claim by Navigil (and not a criminal claim) may be acceptable as Navigil is authorizing the activity (reverse engineering or circumventing protective measures) to improve its system.
- Refrain from disclosing vulnerability details to the public before a mutually agreed-upon timeframe expires.

How to Submit a Vulnerability

To submit a vulnerability report to Navigil's Product Security Team, please send an email to: security@navigil.com.

Preference, Prioritization, and Acceptance Criteria

We will use the following criteria to prioritize and triage submissions.

What we would like to see from you:

- Well-written reports in English will have a higher chance of resolution.
- Reports that include proof-of-concept code equip us to better triage.
- Reports that include only crash dumps or other automated tool output may receive lower priority.
- Reports that include products not on the initial scope list may receive lower priority.
- Please include how you found the bug, the impact, and any potential remediation.
- Please include any plans or intentions for public disclosure.

What you can expect from us:

- A timely response to your email (within 5 business days).
- After triage, we will send an expected timeline, and commit to being as transparent as possible about the remediation timeline as well as on issues or challenges that may extend it.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- Credit after the vulnerability has been validated and fixed.

If we are unable to resolve communication issues or other problems, Navigil may bring in a neutral third party (such as CERT/CC ,ICS-CERT, or the relevant regulator) to assist in determining how best to handle the vulnerability.

This document Version 1.0 was created 22-December-2022

Any updates will be noted below in the version notes.

Version history

2022-12-22 1.0 Initial version