Coordinated Vulnerability Disclosure Policy

Effective Date : 27.05.2024

At Abionic, we consider the cybersecurity of our products of utmost importance. Despite the great care we take regarding cybersecurity, weak points can still remain. If you have found such a weakness, we would like to hear about it as quick as possible so that we can take appropriate measures in the briefest timeframe.

This Coordinated Vulnerability Disclosure Policy outlines the procedures and guidelines for responsible disclosure of cybersecurity vulnerabilities related to Abionic's information systems. We encourage the cybersecurity community and the general public to report any identified vulnerabilities to us in a responsible manner.

Scope

This policy applies to the abioSCOPE device, which is an *in vitro* diagnostic device manufactured by Abionic SA.

How to report a vulnerability

If you believe you have discovered a vulnerability, please send an email to cybersecurity-alert@abionic.com with the subject line "Security Vulnerability Report". When you submit a report, it is important for us to know what product is affected, how the potential vulnerability can be identified, demonstrated, or reproduced, and what type of functional impact the vulnerability allows. Therefore, please provide in your email the following information, if available and/or applicable.

Minimum required information

- description of what product or service is affected;
- Unique Device Identification (UDI) of the abioSCOPE label:
    - (01) ...
    - (11) ...
    - (21) ...
- abioSCOPE software version installed at the time of discovering the vulnerability;
- operating system of involved components;
- time and date of discovery;
- technical description of what actions were being performed and the result in as much detail as possible;
- reporter’s contact information.

Additional information

- sample code that was used to test or demonstrate the vulnerability;
- other parties involved;
- disclosure plans;
- threat/risk assessment details of the identified threats and/or risks including a risk level (high, medium, low) for assessment result;
- software configuration of additional implicated devices at time of discovering the vulnerability;
- relevant information about connected components and devices if vulnerability arises during interaction;
- browser information including type and version information.

After your submission, you will receive an acknowledgment receipt from us within 7 calendar days with a tracking number (vulnerability cybersecurity number) and preliminary information regarding the status of the investigation.

We will contact you in case further information is required from your side.

If a cybersecurity incident impacted or might have impacted patient safety, please send an email to vigilance@abionic.com.

What we expect from you

We expect from you a constructive collaboration with the common aim of promoting safety of the medical devices against cybersecurity risks. We expect that you provide sufficient information to reproduce the problem, so that we will be able to resolve it as quickly as possible.

We also expect that you do not:

- take advantage of the vulnerability or problem you have discovered, for example by accessing more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data;
- disclose the problem to non-implicated third parties until it has been resolved;
- use social engineering, distributed denial of service, spam or applications of third parties.

What you can expect from us

- We will respond to your report within 7 calendar days with our pre-evaluation of the report and preliminary information on the status of the investigation. You will be informed on the process we will follow in order to ensure appropriate analysis and action in response to the reported vulnerability with an estimated timeline.
- If you have followed the instructions above, you will not be subject to any legal action in regard to your report.
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission.
- We will keep you informed of the progress towards resolving the problem.

Release of remediation via vulnerability advisory

Vulnerability advisory and remediations will be communicated via mailing lists to all users/distributors concerned by the vulnerability.

Recognition

We are grateful for your contribution in promoting the safety of our devices against cybersecurity risks. If desired, a special note will be added in the vulnerability advisory to recognise your efforts as a token of recognition for your kind assistance.