Coordinated Vulnerability Disclosure

At Antoni van Leeuwenhoek we work hard to maintain and improve the security of our (medical) devices, systems and services. No matter how much effort we put into system security, there might be vulnerabilities present. If you discover a vulnerability you can report it safely via our *Coordinated Vulnerability Disclosure*, so AVL can take safety measurements.

Reporting a vulnerability

If you have found a vulnerability, we would like to hear about it so that we can take appropriate measures as quickly as possible. AVL is keen to cooperate with you to protect our clients and systems better.

Our Coordinated Vulnerability Disclosure policy is not an invitation to proactively scan our network/ systems for vulnerabilities. We monitor our network/ systems continuously ourselves; Thus, a vulnerability scan is likely to be noticed, investigated upon by our IT department and unnecessary expenses may occur.

If you comply with our Coordinated Vulnerability Disclosure policy we have no reason to take legal action against you regarding the reported vulnerability. We ask you to:

- Send your findings to Z-CERT by sending an email to cvd@z-cert.nl encrypted with our PGP-key. Z-CERT is an organization who handles all cyber security issues on behalf of AVL. Z-CERT will work with you and AVL to make sure that your report is handled with care.
- Provide adequate information to allow Z-CERT to reproduce the vulnerability which helps to resolve the problem as quickly as possible. An IP address or URL of the affected system with a description of the vulnerability will usually be sufficient, although more information might be necessary for more complex vulnerabilities.
- Do not exploit vulnerabilities, e.g. by downloading more data than is needed to demonstrate the vulnerability, looking into third-party data, deleting or modifying data.
- If you suspect to have access to medical data we ask you to let us verify this.
- Do not share information on vulnerabilities until they have been resolved and erase any data obtained through vulnerabilities as soon as possible;
- Do not attack physical security, use social engineering, distributed denial of service, spam, brute force attacks or third-party applications.

How we will handle your report:

- AVL and Z-CERT will treat your report confidentially and will not share your personal data unless required by law;
- Z-CERT will send you an acknowledgement of receipt and will respond to your report with an evaluation and an expected resolution date within 5 working days;
- AVL and Z-CERT will keep you informed of the progress in resolving the problem;
- In communication about the reported problem we will mention your name as the discoverer of the problem (unless you desire otherwise).
- AVL provides a reward by way of thanks. The reward depends on the severity of the vulnerability and the quality of the report.

We strive to resolve any vulnerability as soon as possible. Once the problem has been resolved we will decide in consultation whether and how details will be published.

With thanks to Floor Terra for his sample text in Dutch on http://responsibledisclosure.nl/

[publication date: 19-12-2019]

Out-of-Scope statement

Out of scope

AVL does not reward trivial vulnerabilities or bugs that cannot be abused. The following are examples of known and accepted vulnerabilities and risks that are outside the scope of the responsible disclosure policy:

- HTTP 404 codes/pages or other HTTP non-200 codes/pages and Content Spoofing/Text Injection on these pages.
- fingerprint version banner disclosure on common/public services.
- disclosure of known public files or directories or non-sensitive information, (e.g. robots.txt).
- clickjacking and issues only exploitable through clickjacking.
- lack of Secure/HTTPOnly flags on non-sensitive Cookies.
- OPTIONS HTTP method enabled.
- anything related to HTTP security headers, e.g.:
    - Strict-Transport-Security.
    - X-Frame-Options.
    - X-XSS-Protection.
    - X-Content-Type-Options.
    - Content-Security-Policy.
- SSL Configuration Issues:
    - SSL forward secrecy not enabled.
    - weak / insecure cipher suites.
- SPF, DKIM, DMARC issues.
- host header injection.
- reporting older versions of any software without proof of concept or working exploit.
- information leakage in metadata.