Coordinated Vulnerability Disclosure

At BovenIJ ziekenhuis 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 BovenIJ ziekenhuis 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. BovenIJ ziekenhuis 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 BovenIJ ziekenhuis. Z-CERT will work with you and BovenIJ ziekenhuis 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:

- BovenIJ ziekenhuis 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;
- BovenIJ ziekenhuis and Z-CERT will keep you informed of the progress in resolving the problem;
- BovenIJ ziekenhuis provides a reward by way of thanks. Depending on the severity of the vulnerability and the quality of the report, the reward can vary.

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.

03-03-2021

Not in scope:

BovenIJ ziekenhuis will not process reports of vulnerabilities or security issues that can not be abused or are trivial. Below are a couple of examples of known vulnerabilities and issues that are outside the scope. This does not mean they are not important or should not be resolved, however our CVD process is meant for issues that can be actively abused. For example a vulnerabilities that can be abused by a publicly available exploit or a misconfiguration that can be used to bypass an existing security control. This list of exclusions is derived from a list used by the CERT of Surf (https://www.surf.nl/responsible-disclosure-surf):

- HTTP 404 codes/pages or other HTTP non-200 codes/pages and content spoofing/text injections in these pages
- Fingerprinting/version disclosures of public services
- Public files or directories that do not contain confidential information
- Clickjacking problems that can only be exploited by clickjacking
- No secure/HTTP-only flags on unconfidentional cookies
- OPTIONS HTTP method enabled
- Rate-limiting without clear impact
- All issues related to HTTP security headers, for example:
    - Strict-Transport-Security
    - X-Frame-Options
    - X-XSS-Protection
    - X-Content-Type-Options
    - Content-Security-Policy
- SSL-configuration issues
    - SSL Forward secrecy disabled
- No TXT record for DMARC or a missing CAA-record
- Host header injection
- Reports of outdated versions of any software without a proof of concept of a working exploit