Vulnerability Disclosure Policy

LivAssured BV / Nightwatch is committed to ensure the safety and security of patients, and customers who use our products and services.

Along with the latest advances in information technology, there are also increasing risks regarding security, such as cyber- attacks that exploit vulnerabilities. LivAssured is a company which provides medical devices that affect the health and lives of people living with epilepsy. We are committed to providing our customers with a safe medical device as well as to ensuring security in the operating environment of our medical devices from the viewpoint of our customers. We therefore want to encourage customers, partners, and security researchers who share the same values, to report in a good-faith any digital asset vulnerability they discover.

LivAssured values and appreciates the efforts of security researchers and their reporting, as it helps improve security and reliability. This policy outlines the scope and research covered and the process for reporting vulnerabilities.

Please note that this policy is subject to change, so it should be reviewed regularly.

Scope
As part of the LivAssured Vulnerability Disclosure Policy, the following list of products and services are included:

- All variants of the NightWatch
- Any other products developed by LivAssured| NightWatch

domains and subdomains:

- *.nightwatchepilepsy.com
- *.portal.nightwatchepilepsy.com
- *.nightwatch.nl

If third party products or services are affected as a part of the research, we cannot authorize you to test those. If in doubt, ask us before testing a digital asses, application or platform.

Safe Harbor and privacy
LivAssured promises not to take or support any legal action against any researcher who follows this policy while conducting vulnerability research. This does not apply if recognizable criminal or intelligence intentions are pursued.
If a third party takes legal action against a researcher, even though he was acting in accordance with this policy, LivAssured will ensure that compliance with the policy is communicated. Researchers should submit a report to LivAssured if they have any concerns about compliance before they further proceed with the research. In addition, this policy does not exempt researchers from applicable national, federal, state, and local hacking and privacy laws.

We will keep your report and personal data confidential and share it only to the extent necessary to fix the vulnerability.

Guidelines

Researchers with good intentions and agreeing to the rules pledge to:

- Research only devices and domains within the policy's scope.
- Avoid device or application interruption.
- Respect others' privacy by not destroying, exfiltrating, disclosing or abusing in any other way the data which might become accessible during the research.
- Not exploit any vulnerabilities discovered; advance steps such as persistence, lateral movement, data exfiltration, modification or deletion, code upload etc. are not allowed.
- Not to disclose a vulnerability to third persons or institutions unless fully coordinated with and approved by LivAssured in a written form.
- Not perform any phishing, spamming, social engineering, or denial-of-service attacks.
- Report vulnerabilities promptly to LivAssured.

Reporting Details

Researchers should report vulnerabilities to security@nightwatch.nl
LivAssured promises to acknowledge report submission for the devices and domains in scope by our technical team, after which we will provide feedback to the reporter. Please acknowledge that there is no expectation of payment or compensation and that any future right to claim related to the submitted report is waived

By adhering the following principles, you can enhance the likelihood of your report receiving detailed feedback:

- Provide complete details concerning the affected asset(s).
- Submit a proof of concept, comprising explicit details of the vulnerabilities replication, along with timestamps and screen captures of the problem.
- Elaborate on the reasons why the potential vulnerability could have an impact and to what degree.
- Refrain from submitting automated tool output only