Textmetrics
Oude Oeverstraat 120
6811 JZ Arnhem
+31 26 80 80 191

Responsible Disclosure Policy

At Textmetrics, we believe that the security of our systems, our network and our products is very important. We pay a lot of attention to this during development and maintenance. However, sometimes vulnerabilities escape detection. We appreciate you notifying us if you find one. We would prefer to hear about it as soon as possible so that we can take measures to protect our customers.

This document describes the procedure we have prepared for this.

Reporting

If you believe you've found a security issue in our product or service, please notify us as soon as possible by emailing us at security@textmetrics.com.

Rules

- Do not share information about the security problem with others until the problem is resolved.
- Provide information about how and when the vulnerability or malfunction occurs. Clearly describe how this problem can be reproduced and provide information about the method used and the time of investigation.
- Be responsible with the knowledge about the security problem. Do not perform any actions beyond those necessary to demonstrate the security problem. Do not abuse the vulnerability and do not keep confidential data obtained through the vulnerability in the system.
- Leave your contact details (e-mail address or telephone number) if you want, so that Textmetrics can contact you about the assessment and progress of the vulnerability solution. We also take anonymous reports seriously.
- Do not use physical attacks, DDOS attacks, social engineering or hacking tools such as vulnerability scanners.
- Our responsible disclosure policy is not an invitation to actively scan our company network for vulnerabilities. Our systems are being monitored continuously. As a result, there is a good chance that a scan will be detected and our Security Operation Center (SOC) will investigate it.

How does Textmetrics handle Responsible Disclosure?

When you report a suspected vulnerability in an IT system, we will deal with this in the following way:

- You will receive confirmation of receipt from Textmetrics within three business days after the report.

Textmetrics
Oude Oeverstraat 120
6811 JZ Arnhem
+31 26 80 80 191

- You will receive a response within three business days after the confirmation of receipt containing an assessment of the report and the expected date of resolution. We strive to keep you informed on progress of resolution.
- Textmetrics treat your report confidentially and will not share your information with third parties without your permission, unless this is required by law or by a court order.
- In communication about the reported problem, we will state your name as the party that discovered the problem, if you wish.
- It is unfortunately not possible to guarantee in advance that no legal action will be taken against you. We hope to be able to consider each situation individually. We consider ourselves morally obligated to report you if we suspect the weakness or data are being abused, or that you have shared knowledge of the weakness with others. You can rest assured that an accidental discovery in our online environment will not lead to prosecution.

Exclusions

This Responsible Disclosure scheme is not intended for reporting complaints. The scheme is also not intended for:

- Reporting that the website is not available.
- Reporting fake e-mails (phishing e-mails).
- Reporting fraud.

For issues pertaining to the above and any other inquiries please get in touch with our support team.

Rewards / bug bounty

Textmetrics does not have an active bug bounty scheme. In very exceptional cases a monetary reward can be made available.

Which systems/problems are excluded from rewards?

Not all systems that are accessible under our logos fall under Textmetrics's direct control. Although we also take reports regarding these systems very seriously, we cannot allow them to lead to any rewards.

We also exclude specific problems that in our opinion do not constitute a threat outside of a laboratory set-up.

Textmetrics
Oude Oeverstraat 120
6811 JZ Arnhem
+31 26 80 80 191

EXCLUDED TYPES OF SECURITY PROBLEMS

- SPF / DMARC records
- (D)DOS attacks and rate limiting of calls
- Problems that amount to self-XSS
- Error messages without sensitive data
- Reports from which software we use can be deduced
- Publicly accessible application keys and application secrets in website or mobile application config files
- Problems that require the use of heavily outdated operating systems, browsers or -obsolete plug ins
- Problems that have already been reported by vulnerability scanning tools like Dependabot and Snyk
- Problems that are already known to us

This policy has been drawn up based on the NCSC's Responsible Disclosure Guideline.