Reporting a security vulnerability

Last updated 1 December 2026

Security is at the core of what we do. If you believe you have found a security vulnerability in Spotix, we want to hear about it.

How to report

Email **security@spotix.io** with:

- a description of the vulnerability and where you found it (URL or component);
- the steps needed to reproduce it;
- the potential impact, as you see it;
- your contact details, if you would like us to follow up with you.

Please report in English or Dutch.

What we ask of you

- **Do not test.** We do not invite or authorise security testing of the Spotix platform or its infrastructure. Our Terms of Service prohibit security testing, penetration testing and automated scanning without our prior written consent. This page is a route for reporting vulnerabilities you come across. It is not permission to look for them.
- **If you come across a vulnerability:**
  - do not access, download, modify or delete data, beyond what is unavoidable to notice the vulnerability;
  - delete any data you may have obtained once you have reported;
  - do not use the vulnerability any further;
  - do not attempt to access other users' accounts or our customers' Microsoft 365 or Azure environments.
- **Never** carry out denial-of-service attacks, social engineering, phishing or physical attacks.
- **Keep it confidential.** Do not share the vulnerability with others until we have resolved it.

What we do

- We acknowledge receipt of your report within **five (5) business days**.
- We assess the report and keep you informed of our progress, if you have given us your contact details.
- We aim to resolve confirmed vulnerabilities as quickly as possible, depending on their severity.
- If you wish, we will credit you once the vulnerability has been resolved.

We do not offer financial rewards (bug bounties).

Not in scope

The following are generally not considered vulnerabilities and do not need to be reported:

- missing or "best practice" HTTP security headers without a demonstrated impact;
- SPF, DKIM or DMARC configuration;

- disclosure of software versions or banners;
- missing rate limiting on non-sensitive endpoints;
- clickjacking on pages without sensitive actions;
- reports based solely on the output of automated tools, without a demonstrated exploit;
- vulnerabilities in third-party services that we do not control. Please report those to the provider concerned.

Customers

Customers of Spotix can report suspected security incidents relating to their account in the same way, at security@spotix.io (see section 6.2 of the Terms of Service).

Cloud171 B.V., trading as Spotix · Steenovenweg 5, 5708 HN Helmond, the Netherlands · security@spotix.io