Responsible Disclosures

Have you discovered a vulnerability? Let us know.

At Pon Holdings B.V. and its subsidiaries, we naturally consider the security of our systems and our network to be of the utmost importance. We are convinced that good security is essential to maintain the trust that our clients, suppliers and employees place in us. Despite the care invested in the security of our systems, however, it is still possible that vulnerabilities could be discovered.

By means of our responsible disclosure policy, we ask anyone who has discovered a vulnerability to report it as quickly as possible, so that we can take adequate countermeasures. We would be happy to work with you to solve the vulnerability. Our responsible disclosure policy is not an invitation to actively scan our company network in detail to discover vulnerabilities, as we are already monitoring the network.

We ask that you:

- Report your discoveries as quickly as possible to rd@pon.com. If you would like to encrypt your report before you send it, please inform us in your e-mail and we will give you instructions;
- Provide us with enough information to reproduce the vulnerability, so that we can solve it as quickly as possible. Usually, the IP address or URL for the affected system and a description of the vulnerability is sufficient, but more complex vulnerabilities may require additional information;
- Not to abuse the vulnerability by downloading, viewing, deleting or editing data;
- Not sharing vulnerabilities with others until they can be solved. If you have inadvertently obtained confidential information, then we ask that you delete the data immediately;
- Not to use attacks on the physical security or applications of third parties, social engineering, distributed denial of service (DDoS), spam or disruptive hacking tools.

What can you expect:

- We will always take your report seriously. We will also investigate any suspected vulnerabilities;
- We will reply to your report with our evaluation of the report and an expected date for the solution;
- We will keep you informed of the progress made in solving the vulnerability;
- If you abide by the conditions stipulated above, then we will not take legal action against you pertaining to the report. The Public Prosecutor's Office retains the right to decide whether additional investigation is necessary;
- We will treat your report with confidentiality, and will not share your personal data with third parties without your permission unless required to do so by law, such as when your data are requested by the police or the courts;
- If you submit an anonymous report, we may not be able to contact you with information about the subsequent steps and the progress made in solving the vulnerability;
- We may express our gratitude with a token of appreciation with a value that may vary depending on the severity and the quality of the issue reported. This will be based on the severity of the vulnerability and the quality of the report;
- At your request, we can mention your name as the person who discovered the vulnerability in any communications about the incident;
- We strive to analyse, and if needed solve, any vulnerabilities as quickly as possible after they are discovered. We will also keep all stakeholders informed about the issue.

Non-qualifying vulnerabilities, including but not limited to:

- Flaws affecting the users of out-of-date browsers and plugins. (tabbnabing, etc.)
- Denial-of-service attacks.
- Missing HTTP Security Headers
- Version in HTTP response/Banner Grabbing (without exploitation)
- Clickjacking
- CAA record missing

- OSCP stapling
- Same site scripting
- DMARC/SPF Record Misconfiguration
- HTTP Trace Method
- EXIF metadata in images
- Default webpages with small impact
- Rate limiting vulnerabilities

This *responsible disclosure* policy is based on the Responsible Disclosure Guideline published by the National Cyber Security Centre, and the sample Responsible Disclosure written by Floor Terra.