Process and agreements for reporting a security vulnerability

Coordinated Vulnerability Disclosure

The Shared Service Center ONS (SSC Ons) attaches great importance to the security of its systems. Despite all precautions, it remains possible that a vulnerability can be found in the systems. If you discover a vulnerability in any of our systems, we would like to hear from you so that we can take appropriate action quickly. By making a report, you, the reporter, agree to the terms/provisions below regarding Coordinated Vulnerability Disclosure and the SSC Ons will handle your report in accordance with the aforementioned provisions.

We ask the following of you:

- Email your findings

  Email your findings via secure mail (https://app.zivver.com/security-ssc-ons).

  Please provide us with enough information so we can reproduce the problem and fix it as soon as possible. Usually a description of the vulnerability, the IP address, URL, screenshots and so on of the affected system are sufficient, but more complex vulnerabilities may require additional information to be fixed.
- We welcome tips to help us solve the problem. Please limit your tips to verifiable, factual information that relates to the vulnerability you have identified and avoid giving advice that essentially amounts to advertising specific (security) products.
- Leave contact information so that we can get in touch with you to work together on a secure outcome. Provide at least one email address or phone number.
- Please submit the report as soon as possible after discovery of the vulnerability.

The following actions are not permitted:

- Placing malware, neither on our systems nor on those of others.
- So-called "bruteforcing" of access to systems, except to the extent strictly necessary to demonstrate a serious security deficiency in this area, i.e., if it is extraordinarily easy, using publicly available and readily affordable hardware and software, to crack a password that could seriously compromise the system.
- Using social engineering.

- Disclosing or providing information about the security problem to third parties before the problem has been fixed.
- Taking actions beyond what is strictly necessary to demonstrate and report the security problem. Particularly where it involves processing (including viewing or copying) confidential data to which you have had access due to the vulnerability. Instead of copying an entire database, you can normally suffice with, for example, a directory listing. Modifying or deleting data in the system is never permitted.
- Using techniques that reduce the availability and/or usability of the system or services ((D)DoS attacks).
- Abusing the vulnerability in any (other) way.

What you can expect:

- We treat a report confidentially and do not share a reporter's personal information with third parties without their consent, unless we are required to do so by law or court order.
- We may share the report received (always anonymously) with the partners we work for and the Information Security Service for Municipalities **(Informatiebeveiligingsdienst).**
- By mutual agreement, if you wish, we may mention your name as the discoverer of the reported vulnerability. In all other cases, you will remain anonymous.
- We will send you a confirmation of receipt within 3 business days.
- We respond to a report within 5 business days with an (initial) assessment of the report and possibly an expected date for resolution.
- We solve the security problem you reported as quickly as possible. We strive to keep you well informed of the progress and never take longer than 90 days to solve the problem. We are often dependent on suppliers.
- It can be determined by mutual agreement whether and how the problem will be published after it has been solved.