Coordinated Vulnerability Disclosure (CVD)

policy

Version 3.0 – 21-09-2022

1. Introduction

Hackers who driven by curiosity find vulnerabilities or leaks in the IT-systems of organisations, can often find themselves in a legal grey zone. They may not have bad intentions, but even then it is not always appealing to report the leak to an organisation. Organisations do not always follow up on such reports and sometimes the notifier faces legal consequences. This policy helps to eliminate ambiguities. It states the rules of play to the notifier and explains how Deltion handles the case.

2. Coördinated Vulnerability Disclosure

At Deltion we consider the security of our systems a top priority. However, no matter how much effort we put into system security, there can still be vulnerabilities present. If anyone discovers a vulnerability, we would like to know about it, so we can take steps to address it as quickly as possible, to help us better protect our systems. This policy is published in Dutch and English on the website of Deltion.

What we ask

- Email your findings to csirt@deltion.nl. Encrypt sensitive information to prevent critical information from falling into the wrong hands.
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data,
- Do not reveal the problem to others until it has been resolved,
- Do not use attacks on our physical security, social engineering, distributed denial of service, spam or applications of third parties, or scan our network in any other way to find vulnerabilities. Deltion monitors the network and it is very likely that this is detected, which leads to unnecessary costs.
- Responsible handling of the knowledge about the security problem by not taking any action that goes beyond what is strictly necessary to demonstrate the vulnerabilities.
- Not to perform any harmful actions such as: inserting malware, copying, modifying or deleting data in a system, making changes to the system, repeatedly accessing the system or sharing access with others.

What we promise

- Deltion will not take legal action if the instructions for reporting as stated above, are followed.
- We will respond to the report within five days.
- We will keep the notifier informed of the progress towards resolving the case.
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission, unless we are required to meet legal obligations. It is possible to report anonymous or using a pseudonym.
- In the public information concerning the problem reported, we will state the name of the notifier as the discoverer of the problem (unless he/she desires otherwise).
- We state the name of the notifier in our online Hall of Fame if the notifier appreciates this and we issue a certificate when requested.

We strive to resolve all problems as quickly as possible. Deltion would like to play an active role in the ultimate publication on the problem after it is resolved.

Out of scope

Deltion does not reward trivial vulnerabilities (known and accepted vulnerabilities and risks) or bugs that cannot be abused.

Below are examples of known and accepted vulnerabilities and risks that are beyond the scope of the Coordinated Vulnerability Disclosure policy:

- HTTP 404 codes/pages or other HTTP codes/pages and Content Spoofing/text injection on these pages.
- Fingerprinting/version reference on common/public services.
- Public files or folders containing non-sensitive information, (eg robots.txt).
- Clickjacking and issues that can only be exploited by clickjacking.
- Lack of Secure/HTTPOnly flags on non-sensitive cookies.
- OPTIONS HTTP method enabled.
- Host header injection.
- Anything related to HTTP security headers, for example:
  - Strict-Transport-Security.
  - X-Frame Options.
  - X-XSS Protection.
  - X-Content-Type-Options.
  - Content-Security Policy
- Issues with SSL configurations:
  - SSL forward secrecy disabled.
  - Weak/insecure cipher suites.
- Problems with SPF, DKIM or DMARC.
- Missing DNSSEC information.
- Report outdated software or upgrade possibility without sharing the associated proof of concept of a working exploit.
- Systems and protocols that can be abused for a DDoS attack.
- Intentional directory content listing(s) for research or publishing purposes.
- Information exposure in metadata.

3. Evaluation of policy

Compliance with this policy is monitored periodically. The policy itself is being reviewed by the Privacy and Security Team every two years and adjusted when required.