Responsible Disclosure

English manual

nederlandse
publieke
omroep

June 2019, definitive version
Information Security – among the public with reliable information

Introduction

It is mandatory that the systems of the Dutch Broadcast Organisation (NPO) are safe. That's why we're doing our utmost to ensure a descent, reliable security of those systems. However, it is always possible our security consists of weak spots which could result in vulnerable systems.

By means of a Responsible Disclosure policy, NPO encourage finders of weak spots and vulnerabilities to report them to the NPO. This makes it possible for us to take appropriate measures to correct the finding and reported vulnerability. This implies you are contributing in making and keeping the NPO systems safe.

We ask you to cope responsible with possible findings; the NPO will reward you if you do so. This can be a mention in the NPO Hall of Fame or a small compensation.

How do I report a finding?

- Send an email, as soon as possible after found something, to informatiebeveiliging@npo.nl, preferable encrypted by our PGP Key, published at the NPO site.
- Provide us with sufficient information in order to be able to re-produce your finding. Think of the IP address or the URL of the vulnerable system and a clear description of the found vulnerability. Of course, more complex findings can have a more extensive description. It would be great if you can tell us exactly how we can re-produce the problem.
- Leave us with correct and sufficient contact details: as minimum your name, email-address an a telephone number. We handle your personal information in a responsible manner and in accordance with the NPO privacy policy.
- Confirm written, by email, that you agree with the principles of the NPO Responsible Disclosure policy which require you to handle the vulnerability with responsibility. Refer to the next page.

How do I responsible handle with a finding?

- You do not share information of the found problem and/or vulnerability with others.
- Knowledge about the found problem and/or vulnerability is not being used to things other, an not more than that, demonstrating the problem

The following is prohibited on or via vulnerable NPO systems:

- Spreading of or placing malware, viruses, etc. of any kind.
- Getting repetitive access or sharing access with others.
- Using automated scanning tools.
- Gaining access using brute force attacks.
- Deploying any form of Denial of Service (DoS) attacks.
- Practice social engineering techniques.

What can you expect from the NPO?

Safeguard: You will be safeguarded of legal repercussion if you report a vulnerability in accordance with the NPO Responsible Disclosure policy.

Confidentiality: The NPO handles your reported finding confidential and will not share personal information with others without consent, except if required by law or if a judicial decision is required.

Appreciation: The NPO appreciates your help and we thank you for that, optionally with a reward. Depending on factors such as severity, complexity, quality, etc. of a reported finding, we evaluate which reward fits the situation. This varies from a mention in our Hall of Fame to gift vouchers, with a maximum value of 50 EURO. An important condition is that the reported vulnerability is sever and unknown by the NPO.

Openness and transparency: You will stay informed by the NPO about our evaluation of the finding and the progress of fixing the problem. Of course, we will fix your finding as soon as possible.