Status: Final
Date established by the Executive Board: 02-10-2017
Author: Rianne te Brake

Responsible Disclosure University of Twente

Introduction

The University of Twente considers the security of your and our data very important, which is why we protect our systems. Despite our efforts, a weakness could still occur in this systems.

If you have found a vulnerability in one of our systems, please let us know so that we can take measures as soon as possible. We would like to work with you to better protect our users and our systems.

What we ask of you:

- Not to carry out attacks on physical security or people (social engineering).
- Not to use Distributed Denial of Service attacks or spam.
- Not to report run-of-the-mill issues. Examples of what these are can be found on the cyber safety website under Responsible disclosure.
- To email your findings to responsible-disclosure@utwente.nl. Submitting a notification under a pseudonym is allowed. If you feel the data is so sensitive that you wish to encrypt it, we ask you to notify us in advance. We will then ensure that you are given an email address to which you can send your PGP encrypted email.
- To provide sufficient information for us to reproduce the issue so that we can resolve it as soon as possible. In most cases, it will suffice to provide the IP address or URL of the affected system and a description of the vulnerability, but in the case of complex vulnerabilities, more information may be necessary.
- To delete all confidential information obtained through the breach as soon as possible after reporting it, but always after consulting us to make sure that we can reproduce the issue.
- Not to misuse the problem by downloading more data than necessary to demonstrate the breach, or to inspect, remove or alter third party data.
- Not to share the issue with others until it has been resolved.
- Not to publish anything about the resolved issue unless this has been discussed with us.

What we promise you:

- We feel it is important that vulnerabilities are reported to us as soon as possible, so that we can take immediate action to secure our environment. All notifications will therefore always be gratefully received. We will not consider any legal steps against those who notified us and who gained unauthorized access to sensitive information, if they have complied with the above points.
- We will treat your notification with confidentiality and will not share your personal details with third parties without your consent, unless it is necessary in order to comply with a statutory obligation.
- We will respond to your notification within 5 working days with our assessment of the notification and the date the issue is expected to be resolved.

- We will keep you informed of the progress we make in resolving the issue.
- If you so wish, we will include you as reporter in the Hall of Fame, under a pseudonym if you want.
- We can publish the relevant contents of the resolved issue on www.utwente.nl/en/cyber-safety, unless there are reasons not to do so. That might be the case if the resolved issue has lead to the discovery of a related vulnerability that has not yet been resolved, or when publication could damage the reputation of the University of Twente or one of its units.
- In the publication of the resolved issue, we will credit you, if you wish, as the person who discovered and reported it.

We aim to resolve all reported issues as quickly as possible.