Responsible Disclosure Policy

POLICY

Document information	
Version	1.0
Date	13-10-2023
Document number	1-0062
Author(s)	Security Operations Team
Document owner	CISO

1. Introduction

Security at Eindhoven University of Technology (TU/e) is a very high priority, and we take a lot of care in maintaining and safeguarding our systems, network, users and TU/e data. However, despite the care, sometimes some vulnerabilities are inadvertently left in the systems/network or are newly introduced due to the ever-evolving nature of the software and hardware used. This policy is intended for all the parties, both internal and external to TU/e, and it delineates the responsibilities, DOs and DON'Ts, scope and legal implications.

2. Purpose

At TU/e, responsible disclosure of the vulnerabilities mentioned above, by ethical external parties/researchers, internal TU/e staff, researchers and students is appreciated. If you find a weak spot in one of our systems, we request you to 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, data and our systems.

However, please note that our responsible disclosure policy is not an invitation to actively scan our university network extensively to discover vulnerabilities. We monitor our network constantly. As a result, your scan(s) will be picked up by our Computer Emergency Response Team (CERT) which might also in turn incur unnecessary costs.

3. Policy guidelines

During your investigation it could be possible that you might take actions that are prohibited by law. If you follow the conditions given in this policy, we will not take legal action against you. However, the Public Prosecutor always has the right to decide whether or not to prosecute you.

DOs and DON'Ts:

- Please mail your findings as soon as possible to cert@tue.nl. Preferably encrypt your findings with our PGP key to prevent the information from falling into the wrong hands. PGP encryption is not mandatory. The PGP key can be found in our security.txt file here.
- Don't abuse the found vulnerability, for example:
    - downloading more data than necessary
    - changing or removing data
- Be extra cautious and show extra restraint with Personal Identifiable Information (PII Data)
- After finding a vulnerability, don't continue to exploit it to find data or other internal information, or additional vulnerabilities as an extension using the initial vulnerability.
- Do not share the vulnerability with others until it is resolved
- Do not test the physical security or third-party applications, social engineering techniques, (distributed) denial-of-service, malware, or spam.
- Be as verbose and in detail as possible about the vulnerability and provide any evidence you might have. Be assured that your notifications will be received by specialists of the CERT team of TU/e.
- Do provide sufficient information to reproduce the problem (i.e., Steps to Reproduce) so that we can resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a

description of the vulnerability is sufficient, but complex vulnerabilities may require further explanation.

TU/e's Next Steps:

- If a valid disclosure is submitted, we will respond to your report within 5-7 business days with our evaluation of the report and an expected resolution date.
- We will keep your report anonymous and will not pass on your personal details to third parties without your permission, unless the law requires us to provide your personal information.
- We will keep you informed of the progress towards resolving the problem.
- You can report anonymously or under a pseudonym. In this case, however, we will not be able to contact you for things such as follow-up steps, progress of resolving the issue, publication or any letter of appreciation for reporting.
- We may add you to our Hall of Fame for your research but are not obliged to do so. You are, therefore, not automatically entitled to enlistment. The enlistment happens on a case-by-case basis. Whether to add to the Hall of Fame and in what detail and form depends on the care taken in your investigation, the quality of the report and the seriousness and complexity of the leak.
- We strive to solve all problems as quickly as possible and keep all parties involved informed.

4. Scope

TU/e does **NOT** recognize trivial vulnerabilities or bugs that are difficult to abuse. The following are examples of known and accepted vulnerabilities and risks that are not in scope of this policy:

- HTTP 404 codes/pages or other HTTP non-200 codes/pages and Content Spoofing/Text Injection on these pages.
- Fingerprint version banner disclosure on common/public services.
- disclosure of known public files or directories or non-sensitive information, (e.g. robots.txt).
- clickjacking and issues only exploitable through clickjacking.
- lack of Secure/HTTPOnly flags on non-sensitive Cookies.
- OPTIONS HTTP method enabled.
- anything related to HTTP security headers, e.g.:
    - Strict-Transport-Security.
    - X-Frame-Options.
    - X-XSS-Protection.
    - X-Content-Type-Options.
    - Content-Security-Policy.
- SSL Configuration Issues:
    - SSL forward secrecy not enabled.
    - weak / insecure cipher suites.
    - host header injection.
- SPF, DKIM, DMARC issues.
- reporting older versions of any software without proof of concept or working exploit.
- information leakage in metadata.

- Responsible disclosure notifications about the websites of students, (student) associations, and start-up companies hosting their websites. Although these sites are on the university's network, they are not the responsibility of the university. Responsible disclosure notifications about these sites may or may not be forwarded to the responsible parties. These reports do not result in an entry into the Hall of Fame, and no updates on progress are provided.

In addition, reports that can be considered a beg bounty will neither be processed nor responded to.

5. Hall of Fame

TU/e does not provide a monetary bounty. We can, however, add your name to our Hall of Fame with a link to your online profile. Please note that this only applies to the first person reporting a specific unique vulnerability. You can find our Hall of Fame here.