Responsible Disclosure Policy House of Trust

Version: 1.0
Date: September 26th 2024

House of Trust B.V.
Veenweg 71 H
1701 HC Heerhugowaard

E-mail: info@houseoftrust.nl
BTW-nr: NL866936774B01

KvK: 94919720
IBAN: NL97ABNA0137041578

Version control

Date	Version	Change	Author
26.09.2024	1.0	First Draft	Mr. Lennert D. Ouwerkerk (LL.M.)
14.10.2024	1.1	English version	Wiebe Woudstra

Table of contents

Scope

This Responsible Disclosure Policy is written for the private limited company's systems:

- House of Trust B.V.

Introduction

At House of Trust, we consider the security of our systems very important. Despite our concern for their security, it is possible that there is still a weak spot.

If you find a weak spot in one of our systems, please let us know as soon as possible so that we can take measures. We want to work with you to better protect our customers and systems.

Please note that this Responsible Disclosure policy does not invite us to actively scan our corporate network extensively to discover vulnerabilities. We continuously monitor our network ourselves. As a result, there is a good chance that a scan will be picked up and that any problems will be investigated by our CERT (Computer Emergency Response Team), preventing unnecessary costs.

We ask you:

- E-mail your findings to info@houseoftrust.nl.
- Not to exploit the problem by, for example, downloading more data than is necessary to demonstrate the leak or viewing, deleting or modifying data from third parties;
- Do not share the problem with others until it is resolved, and delete all confidential data obtained through the leak immediately after the leak has been patched;
- Use attacks on physical security, social engineering, distributed denial of service, spam, or third-party applications, and
- Please provide enough information to reproduce the problem so we can fix it quickly. Usually, the affected system's IP address or URL and a vulnerability description are sufficient, but more complex vulnerabilities may require more.

What we promise:

- We will respond to your report within three (3) days with our review of the report and an expected resolution date;
- If you have complied with the above conditions, we will, in principle, not take any legal action against you regarding the report; we explicitly say "in principle" here because we want to reserve the right to take legal action if, for example (i) how you discovered the problem is not related to your skills, but is related, for example, to the use of illicit or illegal software; (ii) you have hired a company or people to discover the problem; (iii) you raise the issue to blackmail us; and (iv) you were hired and paid by a third party to discover the problem;

- We treat your report confidentially and will only share your data with third parties with your permission, if necessary, to comply with a legal obligation. Reporting under a pseudonym is possible;
- We will keep you updated on the progress of resolving the issue;
- In reporting on the reported problem, we will, if you wish, mention your name as the discoverer and
- As a thank you for your help, we offer a reward for every report of a security issue that is unknown to us. We determine the size of the reward based on the severity of the leak and the quality of the report; we do not give a reward for problems that cannot be exploited (see below – next heading);
- We aim to resolve all issues as quickly as possible and would be happy to be involved in any publication about the issue after it has been resolved.

In any case, what is not seen as a vulnerability:

- HTTP pages with return code 404 or other codes that are not 200;
- version indication of the software used;
- open directories with insensitive content;
- no secure flag or HTTPS-only flag on insensitive cookies;
- problems with SPF, DKIM, DMARC, or other DNS records;
- domain names without DNSSEC;
- or reporting outdated versions of software without demonstrating a working vulnerability.

This document is based on the sample document, which appears at http://www.responsibledisclosure.nl/. That sample document was written by Floor Terra and is published under a Creative Commons Attribution 3.0 license. According to the text of the website cited, this sample document was created in part thanks to feedback from and discussion(s) with Deloitte, Rickey Gevers, Oscar Koeroo, Ronald Prins (Fox-IT), @JeroenSlobbe, NCSC, @WhatSecurity and others.

We have changed that sample document to make it meet our requirements and wishes.