COORDINATED VULNERABILITY DISCLOSURE POLICY

Classification: Public
Version: 1.0

CONTENTS

1 COORDINATED VULNERABILITY DISCLOSURE POLICY

1.1 Introduction

Thank you for taking the time to read our coordinated vulnerability disclosure policy! Eurofiber takes the security of its systems very seriously. Despite the fact that we do our best to secure our systems to the extent of our capabilities, it is still possible that there is a weak spot in our systems. This policy describes the procedure to follow and what to expect after you report a vulnerability in our systems to our teams.

If a vulnerability is found in one of our systems, we would like to know as soon as possible, so we can take the appropriate measures to resolve this vulnerability. To this end, Eurofiber would like to work with ethical hackers to better secure our systems.

1.2 Scope definition

Coordinated vulnerability disclosure concerns all Eurofiber systems that can be accessed from the public internet. These can be systems that are publicly visible by default or unconsciously. Eurofiber takes care of monitoring its internal systems for vulnerabilities. Third-party systems are outside the scope of this policy.

1.3 Rules of engagement

Eurofiber appreciates all efforts of finding, possibly exploiting and reporting a vulnerability in our systems. We therefor introduce these rules of engagement to help you with the reporting process.

1.3.1 Scanning

These rules of engagement are no invitation to actively and progressively scan our network or systems for weaknesses. Our network is actively monitored and we want to prevent unnecessary scanning on our systems. We also understand that scanning is a part of the reconnaissance stage and therefor sometimes trivial in finding weaknesses. We urge you to tread lightly when doing so.

1.3.2 Ethical hackers

Ethical hackers that have found vulnerabilities in our systems are invited to inform us about these vulnerabilities.

- Please send us an email at servicedesk@eurofiber.com with a brief description of the finding;
- Leave your contact details so that we can contact you if necessary. That allows us to work together towards a solution. At least one email address or phone number is mandatory;

- Please do not abuse the vulnerability. Do not download more data and do not dig further than necessary to prove the vulnerability. In addition, it is not permitted to view, modify or delete data. Additional restraint is also expected with personal data;
- Please do not share data that has been acquired to prove the vulnerability with others;
- Please confirm to us that you did not distribute this data and deleted the data when the vulnerability is reported to us, data needed to replay the attack must be removed after the vulnerability is resolved;
- Please do not share the vulnerability with others until it is resolved. If the vulnerability is CVE worthy we will assist you in getting it CVE numbered via the appropriate authorities and scoring mechanisms;
- Please provide sufficient information to reproduce the vulnerability so that we can solve it as quickly as possible. In many cases, the IP address or URL of the affected system is sufficient, but more complex vulnerabilities may require more information, if this is the case we will inform you;
- We are open to tips that can help us solve the vulnerability. However, please note that the advice is based on verifiable facts and does not amount to advertising for certain products.

1.3.3 Eurofiber

- We will send a confirmation of your findings within 5 working days after receipt of the findings. We strive to follow up on the assessment of the report and next steps within 10 working days. Depending on the complexity of the vulnerability, we will of course keep you informed of our follow-up progress;
- If you as reporter have complied with the conditions indicated in 1.3, we will not take legal action regarding the report;
- If needed, Eurofiber will provide a storage medium where additional files can be shared for further analysis;
- In reporting on the reported vulnerability, we will, if you so desire mention you as the discoverer;

2 REWARDS

We may offer a reward as a thank you for reporting the vulnerability in accordance with this policy. Depending on the severity of the vulnerability and the quality of the notification, the reward may vary from a simple "Thank you," to a sticker or a T-Shirt. In any case, the reporter receives an entry in the Hall of Fame. No financial rewards are given. Please refrain from claiming a financial reward. E-mails containing a claim for a financial reward will be ignored.

We strive to solve all vulnerabilities as quickly as possible, and we are willing to cooperate in any publication about the vulnerability after it has been resolved.

3 EXCEPTIONS

Eurofiber does not respond to non-trivial vulnerabilities or bugs. These findings can be reported to us but we will most likely not respond to them.

Below are some examples of vulnerabilities and accepted risks that we consider to be outside of the scope of the coordinated vulnerability disclosure policy:

- HTTP 404 codes/pages or HTTP non-200 codes/pages and content spoofing/text injecting on these pages
- Output automated tool scans. Examples: Web, SSL/TLS scan, Nmap scan results, etc.
- Public files or directories with non-sensitive information (e.g. robots.txt)
- Clickjacking and vulnerabilities that can only be exploited via clickjacking
- No secure/HTTP-only flags on non-sensitive cookies
- OPTIONS HTTP method enabled
- Everything related to HTTP security headers, for example:
    - Strict-Transport-Security
    - X-Frame-Options
    - X-XSS-Protection
    - X-Content-Type-Options
    - Content-Security-Policy
- SSL-configuration issues:
    - SSL Forward secrecy disabled
    - Weak/insecure cipher suites
- SPF, DKIM of DMARC issues
- Host header injection
- The use of third-party scanning tools/methods to create a disruption in our services, using these methods can result in legal steps.
    - DDOS
    - Phishing
    - Spam
- Reports of outdated versions of software without a proof of concept or working exploit

4 THANK YOU!

First and foremost, thank you for your efforts to keep Eurofiber, our systems and there for our customers and the world a safer place. We appreciate your efforts and recognize the level of technical skill needed to perform these activities.