PUBLIC, NO LIMIT ON DISCLOSURE

Vulnerability Disclosure

Table of contents

1.0 Introduction

EPI highly values the security of its systems and platform, and the effort security researchers put in to improve it.

Even though we continuously take the utmost care of our systems, it might just happen that you have found a vulnerability or weakness. To resolve this swiftly, we kindly request that you follow this guideline to report it to us.

2.0 Scope

Only EPI (EPI SE and EPI Ops BV) owned and administered services are in the scope of this policy. This includes:

- EPI affiliated web domains like epicompany.eu, wero-wallet.eu and other EPI domains,
- Payment systems and APIs operated by EPI including EPI Central Services domains and Wero back-office systems.
- iOS and Android apps of EPI.

3.0 Policy

If a security researcher makes a good faith effort to comply with this policy during the security research, EPI will consider the research they perform to be authorized by EPI. EPI will work with the researcher to understand and resolve the issue quickly, and EPI will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this disclosure, we will make this authorisation known.

3.1 Not authorized testing methods

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests, application denial of service tests, or other tests that impair access to or damage a system or data.
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical or physical vulnerability testing.

3.2 Guidelines

To encourage disclosing your report responsibly, we will not take legal action against you nor ask law enforcement to investigate you, and possibly reward you, provided that you comply with these guidelines:

- Send the details in an email to security@epicompany.eu to report any vulnerability you've discovered promptly.
- Make a good faith effort to prevent privacy violations, destruction of data and interruption/degradation of any of our services. In particular, if a vulnerability allows unintended access to data: limit the size of data you access to the minimum required for effectively showcasing a Proof of Concept.
- Avoid all forms of extortion.
- Do not download, read, share or modify any information or data that does not belong to you.
- Do not share details that relate to the vulnerability with others until fully mitigated.
- Destroy all remaining private data, resulting from your research, immediately after reporting the vulnerability.
- Do not use any research attempt that involves breaching or attacking physical security or the use of social engineering, DOS, spam, fishing or any involvement of third parties.
- Provide details of the vulnerability so that we can reproduce it, including a Proof of Concept (PoC), information on the URL, endpoint and IP address, and other necessary information. Allow us to respond and mitigate within a reasonable amount of time.

Note that you will still have to abide by any applicable law and that potential law enforcement consequences are not within our control.

3.3 EPI's commitment & expectation

EPI will put effort to

- respond within 3 business days,
- handle your report and personal details with utmost confidentiality,
- keep you posted on the progress,
- reward you in cases of serious and unknown vulnerabilities, containing enough information to swiftly reproduce.

Note that people who are in any way involved with designing, regulating, auditing, creating or maintaining our services or platform are not eligible for reward.

3.4 Out of scope

The following is specifically out of scope and not eligible for reward either:

- reports without a clear description of the vulnerability and of of potential exploits,
- vulnerabilities concerning other sites and domains not affiliated with EPI,
- CSFR issues on public and non-authenticated web pages,
- the absence of best practice security headers, like HSTS, HttpOnly, CSP, XSS or click-jacking related headers,
- possible old/vulnerable third party/off-the-shelf systems without evidence that they are exploitable and impacting the security of EPI services,
- TLS/SSL related configuration issues,
- findings for webpages, APIs and mobile apps operated and provided by EPI Scheme members, but not by EPI.

3.5 Safe Harbour

When performing good-faith vulnerability research in line with this disclosure and relevant legal contracts, such research is deemed:

- Legal under anti-hacking laws.
- Legal under anti-circumvention laws.
- We will not sue for bypassing lawful technology controls.
- Beneficial to overall internet security, conducted in good faith.

Always adhere to all applicable laws. If a third party sues you, but you've followed this disclosure, we'll support your compliance. If you're unsure about your research's alignment with this disclosure, submit a report via official channels.

Please note: this Safe Harbor only covers claims managed by the disclosures participating organization, not independent third parties. It's not valid if you breach this disclosure or our Terms of Service, even unintentionally.

.