Strathclyde Partnership for Transport

Vulnerability Disclosure Process

Page	Version	Date	Purpose/Changes	Initials
All	0.1	24/07/2024	Draft Policy	DC
All	1.0	24/07/2024	Review and approval	CT

Contents

1. Introduction

This vulnerability disclosure process applies to any vulnerabilities you are considering reporting to Strathclyde Partnership for Transport ("SPT") so long as SPT's website has a published security.txt file that references this process.

We recommend reading this vulnerability disclosure process fully before you report a vulnerability and always acting in compliance with it.

We value those who take the time and effort to report security vulnerabilities according to this process. However, we do not offer monetary rewards for vulnerability disclosures.

2. Reporting

If you believe you have found a security vulnerability relating to the SPT's systems, please submit a vulnerability report to the address defined in the CONTACT field of the published security.txt file.

In your report please include details of:

- The website, IP or page where the vulnerability can be observed.
- A brief description of the type of vulnerability, for example; "XSS vulnerability".
- Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.

3. What to expect

After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 10 working days. We'll also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports may take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This maximises the time our technologists or suppliers have to focus on remediation.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Once your vulnerability has been resolved, we welcome requests to disclose your report. We'd like to unify our guidance, so please do continue to coordinate public release with us.

4. Guidance

You must NOT:

- Break any applicable law or regulations.
- Access unnecessary, excessive or significant amounts of data.
- Modify data in the SPT's systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.
- Disrupt SPT's services or systems.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with "best practice", for example missing security headers.
- Submit reports detailing TLS configuration weaknesses, for example "weak" cipher suite support or the presence of TLS1.0 support.
- Communicate any vulnerabilities or associated details other than by means described in the published security.txt.
- Social engineer, 'phish' or physically attack SPT's staff or infrastructure.
- Demand financial compensation to disclose any vulnerabilities.

You must:

- Always comply with data protection rules and must not violate the privacy of any data the SPT holds. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

5. Legalities

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause SPT or partner organisations to be in breach of any legal obligations