Loop Software Vulnerability Disclosure

OVERVIEW

This policy sets out the procedure in which security researchers can report potential security vulnerabilities to Loop Software responsibly and ethically.

Maintaining the utmost level of security is our top priority and therefore we take many steps to keep our systems and customers secure. Despite this, there still may be vulnerabilities within the Daymap product and other related services.

We appreciate the assistance from security researchers and are committed to reviewing the reports which are disclosed to us promptly. If you believe that you have discovered a potential security vulnerability in a Daymap product or related system, please contact us as quickly as possible. We request that security researchers are patient and provide us with a reasonable and proportionate timeframe to address the issue.

Strictly, do not publicly disclose details of any potential security vulnerabilities without expressed consent from the security delegate at Loop Software.

Compensation is not assured for finding potential or confirmed vulnerabilities. Although compensation may be considered at the discretion of Loop Software for confirmed vulnerabilities. Research should not be conducted with the belief of receiving monetary compensation for findings.

Loop Software will not initiate legal action against researchers as long as their efforts are in good faith, and strictly in adherence to this policy. In the event of non-compliance, we reserve all of our legal rights.

This policy may be updated at any time for any reason.

SCOPE

All testing by researchers must be conducted strictly in scope. Researching out of scope is strictly forbidden.

a. Sites & Services in Scope

- Web properties owned and operated by Loop Software, which are completely unaffiliated with any Education organisation or Loop Software customer, are in scope.

b. Sites & Services out of Scope

- Customers of Loop Software (and their web services) are out of scope.
- Web properties Loop Software operates on behalf of a customer are also out of scope.
- 3rd party services/integrations are also out of scope.

RESEARCH CONDITIONS & ISSUE REQUIREMENTS

Loop Software does not allow certain types of security research. Conducting prohibited research is not in accordance with this policy. Excluded research/vulnerabilities should not be reported unless they are

believed to be particularly (or abnormally) harmful.

a. Prohibited Research Types

- Conducting social engineering (including phishing) against Loop Software employees or Loop Software customers (including system admins).
- Executing or attempting to execute denial of service attacks (DoS).
- Any physical attacks on-premises (including but not limited to Loop Software offices and data centres).
- The use of automated vulnerability scanners.
- Any activity that violates any law.
- Testing applications or services that integrate into Daymap.
- Linking, injecting, or uploading harmful payloads (including exploiting cross-site scripting vulnerabilities with payloads intended to cause harm or uploading malware or spyware).
- Data exfiltration of sensitive personal information under any circumstance.
- Accessing (or attempting to access) sensitive personal information.

b. Excluded Research/Non-Qualifying Issues

- Any security issue that does not have a valid attack scenario.
- Use of vulnerable libraries or frameworks without a valid attack scenario.
- Attacks that rely on outdated/unpatched browsers or platforms.
- Descriptive Error Messages (including stack traces, or other errors).
- HTTP non-200 codes.
- CSRF with minimal security implications.
- Missing 'Secure' or 'HTTPOnly' flags on non-sensitive cookies.
- Missing HTTP headers.
- Weak or insecure SSL ciphers and certificates.
- Clickjacking attacks (and attacks alike).

PROCESS

To responsibly disclose potential security vulnerabilities, please email *security@daymap.net*. Ensure you have read and understood this policy thoroughly before contacting us.

When disclosing a potential security vulnerability, please disclose as much information as possible. Well-written English is the best way to communicate with us.

a. Information to Include in Responsible Disclosure

- A detailed explanation of the potential security vulnerability.
- An attack scenario of the vulnerability.
- Steps to reproduce the vulnerability, with proof-of-concept code (where applicable).
- A list of services that may be affected.
- Your contact information.

b. What to Expect from Loop Software

- A timely response to your disclosure (within 2 business days).
- An open dialogue to discuss issues.
- Updates on the progress of your report.

c. Ongoing Requirements for the Security Researcher

- Maintain confidentiality and do not disclose details of the reported vulnerability.

Please note, as previously stated, compensation is not assured for any disclosure of vulnerabilities (including confirmed vulnerabilities).