Vulnerability Responsible Disclosure policy

1. Overview

1.1 Purpose

Batopin NV is committed to provide secure systems and services to the general public by implementing appropriate security measures and processes to protect the information it handles. While we strive to maintain a high level of security, vulnerabilities may still be present.
The purpose of this policy is to provide anyone with the relevant skills a clear framework for responsibly identifying and reporting potential security vulnerabilities. It also defines the process for submitting vulnerability information to Batopin NV, enabling us to investigate, validate and address reported security issues.

1.2 Scope

This Policy applies to all information security vulnerabilities identified by third parties in:
• public-facing ATM interfaces operated by Batopin
• cash.be
• batopin.be
Other systems managed or used by Batopin are explicitly out of scope and are not authorised for testing under this policy.

2. Vulnerability Disclosure Policy

2.1 Investigation

Provided that you act in good faith, comply with the scope, conditions and restrictions of this policy, and comply with all applicable laws and regulations, Batopin does not intend to pursue legal action against you in relation to your vulnerability investigations.

2.1.1 General conditions

The following conditions must be complied with when performing a security investigation on the permitted systems:

- Notify Batopin as soon as possible after you have identified a security vulnerability;
- Do not exploit vulnerabilities beyond what is strictly necessary to demonstrate the vulnerability. Proportionality must be maintained: if the vulnerability can be demonstrated on a small case, no further action should be taken;
- Do not share access with anyone;
- Immediately stop testing and report the vulnerability if customer information, personal data, authentication credentials, transaction data or other confidential information becomes accessible;
- Testing must be performed in a manner that avoids disruption, degradation or interruption of Batopin's services and systems;
- Any backdoors, access and persistence must be removed after the vulnerability has been demonstrated.

2.1.2 Forbidden actions

The following actions are strictly prohibited during the investigation:

- Accessing, processing or copying data, unless to the extent strictly necessary to perform your investigation. After the investigation, the data must be destroyed permanently;
- Altering, deleting or otherwise damaging data and systems;
- Installing malware;
- Any techniques with the sole purpose of impacting the availability of our systems and services, such as (Distributed) Denial of Service ((D)DOS) attacks, load testing and stress testing;
- Any attempts to bypass the physical security controls;
- Social engineering and phishing attacks;
- Spamming;
- Stealing passwords or brute force techniques;
- Vandalism;
- Any attempts to dispense cash, alter transactions, interfere with transaction processing or otherwise impact the financial operations.

2.1.3 Confidentiality

Third parties must treat all information obtained during the investigation as strictly confidential, and must not share, disclose or otherwise use such information for any purpose other than reporting the vulnerability to Batopin.

In the event that the vulnerability may also affect other organisations in Belgium, the third party responsible may inform the Center for Cybersecurity Belgium without revealing any detailed Batopin information.

Public disclosure, publication, discussion on social media, conference presentations or sharing vulnerability details with other parties is not permitted unless Batopin has confirmed remediation or provided prior written authorisation.

After remediation has been confirmed by Batopin or where prior written authorisation is obtained, the reporter may publicly disclose the existence of the vulnerability, provided that:

- Batopin is informed in advance of the intended disclosure;
- The disclosure does not contain exploit code, proof-of-concept code, detailed attack instructions, configuration details, screenshots or any other information that could reasonably facilitate exploitation of the vulnerability;
- No confidential information, personal data, customer information or other security-sensitive information relating to Batopin is disclosed;
- The disclosure complies with all applicable laws and regulations.

2.2 Reporting

Third parties, including security researchers and ethical hackers, are encouraged to report identified vulnerabilities to security@batopin.be. Reports may be submitted anonymously. When contact details are shared, receipt of your submission will be acknowledged.

Upon request by the third party, Batopin will provide a secure link through which the vulnerability report can be uploaded to a secure location managed by Batopin.

When reporting a vulnerability, we kindly recommend providing:

- A description of the vulnerability
- Steps to reproduce the issue (scripts or screenshots are helpful)
- Potential impact
- Location of the vulnerability

May we ask to submit reports in English.

To the best of Batopin’s ability and where permitted by law, Batopin will confirm the existence of the vulnerability.

Batopin aims to:

- Acknowledge receipt of vulnerability reports within 5 business days;
- Perform an initial assessment of the report;
- Provide updates where appropriate during the investigation;
- Engage with the reporter where additional information is required.

These targets are indicative and do not constitute binding commitments.

2.3 Rewards

Batopin does not currently operate a vulnerability reward or bug bounty program. Batopin may, at its sole discretion, provide recognition for valid reports. Any such recognition is not guaranteed and is assessed on a case-by-case scenario.

2.4 Questions

Questions regarding this policy may be sent to security@batopin.be. We also invite you to contact us with suggestions for improving this policy.