Responsible Disclosure – reporting security vulnerabilities

We at BAWAG Group take compliance and security of our products, services and data very seriously. If you have found an issue or a cybersecurity vulnerability in one of our applications, we would like to hear from you through our responsible disclosure process. We believe that responsible disclosure of any security vulnerability identified by security researchers is an essential part of the commitment to ensure stringent quality standards of our security.

This Responsible Disclosure Policy ("Policy") gives security researchers clear guidelines for conducting acceptable vulnerability discovery activities and how to submit discovered potential vulnerabilities to us.

Responsible disclosure requires mutual trust, respect, and transparency between involved parties. If you believe you have found a real or potential security vulnerability in any BAWAG Group offered service or software, then please report it to us as soon as possible at disclosure@bawaggroup.com. We would like to work with you to protect our systems and services more effectively.

Scope

All publicly available / reachable Internet based services and solution offerings (including Apps) of BAWAG Group are in scope.

Proposed Disclosure Process

- We prefer all communications to be in English or German.
- Please DO NOT disclose or report the vulnerability to third parties until
    - we have been able to correct it and
    - we have given our written consent
- Please report potential vulnerabilities to the BAWAG Group Security team at disclosure@bawaggroup.com.
- Please include the requested information listed below (as much as you can provide) to help us better understand the nature and scope of the possible issue:

    - Type of issue (e.g. SQL injection, cross-site scripting, RCE, SSRF, etc.);
    - Full paths of (source) file(s) related to the manifestation of the issue;
    - When applicable, the location of the affected source code (tag/branch/commit or direct URL);
    - Any special configuration required to reproduce the issue;
    - Step-by-step instructions to reproduce the issue;
    - Impact of the issue, including how an attacker might exploit the issue. This information will help us triage your report more quickly.
- Please do not submit a high volume of low-quality reports on security vulnerabilities (e.g. re-posting of vendor notices for platform updates).
- We will acknowledge receipt of your vulnerability report as soon as possible.
    - In case your vulnerability report is a 'valid issue' then we will strive to send you regular updates about our progress.
    - If for some reason you do not receive a response within a reasonable time from us, then please follow up via eMail to ensure we received your initial message.
- You may publish information about the vulnerability on social platforms, in public or to any third party, only after
    - the vulnerability has been fixed and
    - with our prior written approval by notifying us at least one month in advance.
- Hence, you can identify us in public or before any third party only after giving our explicit written approval.

Rules of Engagement

- Please always ensure to avoid any impact on the proper functioning of the system, both in terms of availability and performance, but also in terms of confidentiality / privacy and integrity of the data.
- Do not use attacks on physical security, spam, social engineering (phishing, vishing, spam, etc.), distributed denial of service or third-party applications.
- Please only use exploits to the extent necessary to confirm the presence of any real or potential security vulnerability and do not

use an exploit to compromise or exfiltrate data, establish persistent command-line access, or use the exploit to pivot to other systems.

- Do not apply the following actions:
  - Placing malware (virus, worm, Trojan horse, etc.);
  - Copying, modifying, or deleting data in a system;
  - Making changes to the system;
  - Using automated scanning tools; (e.g. Nessus, Burpscan Report, etc.)
  - Using the so-called “brute force” method of access to systems;
  - Using denial-of-service / DoS
  - Sharing access with others;
- Do not exploit the vulnerability by unnecessarily copying, deleting, adapting or viewing data. Or, for example, by downloading more data than is necessary to demonstrate the vulnerability.
- Please erase all obtained/exfiltrated data as soon as it is reported.

Acknowledgements

We are not offering cash rewards for any detected vulnerability.

Final Notes

Acts under this Policy should be limited to identify potential vulnerabilities and sharing this sensitive information with BAWAG Group.

If you have any questions, we encourage you to address them to the BAWAG Group Security team at disclosure@bawaggroup.com. In case of doubt about the applicability of this Policy, please contact us first via the above-mentioned eMail address, to ask for clarification.

BAWAG Group reserves the right to change the content of this Policy from time to time or to terminate the Policy at any time.