Vulnerability Disclosure Policy

This is the qiio AG ("qiio", "we" or "us") Security Vulnerability Disclosure Policy and applies to any vulnerabilities you are considering reporting to us.

1. Introduction

We actively endorse and support working with the research and security practitioner community to improve our online security. We have developed this vulnerability policy to reflect our company values and to uphold our legal responsibility to good-faith security researchers that are providing us with their expertise.

We welcome investigative work into security vulnerabilities, carried out by well-intentioned and ethical security researchers. We are committed to:

- investigating and resolving security issues in our platform and services thoroughly
- working in collaboration with the security community
- responding promptly and actively

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting qiio. We recommend reading this vulnerability disclosure policy 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 policy. However, we do not offer monetary rewards for vulnerability disclosures.

Please note that this page does not provide any form of indemnity for any actions if they are either in breach of the law or of this policy. It does not provide an indemnity from qiio or any third party.

2. Scope

This disclosure policy applies only to vulnerabilities in qiio products and services under the following conditions:

- 'in scope' vulnerabilities must be original, previously unreported, and not already discovered by internal procedures
- volumetric vulnerabilities are not in scope, meaning that simply overwhelming a service with a high volume of requests is not in scope
- reports of non-exploitable vulnerabilities, or reports indicating that our services do not fully align with "best practice", for example missing security headers, are not in scope
- TLS configuration weaknesses, for example "weak" cipher suite support or the presence of TLS1.0 support, are not in scope

The policy applies to everyone, including, for example: qiio staff, third party suppliers and general users of qiio's products and services.

3. **Bug bounty**

We do not offer a paid bug bounty program. We will, however, make efforts to show our appreciation to security researchers who take the time and effort to investigate and report security vulnerabilities to us according to this policy wherever we can.

4. **Reporting a vulnerability**

If you believe you have found a security vulnerability, please fill out the form on the qiio.com/security website.

In your report, please include details of:

- positive confirmation that you have read & understood the Vendor's Vulnerability Disclosure Policy
- a brief description of the type of vulnerability, for example "XSS vulnerability"
- name of the affected product/service, plus specific version number, model number, serial number etc.
- any Proof of Concept (PoC) setup details
- description of steps to reproduce the issue:
    - 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
- perceived impact and severity if the vulnerability were to be exploited
- any perceived impact on other products, services, vendors etc.
- any intended further actions you want to take, and expectations from qiio
- other relevant information

5. **What to expect after submitting a report**

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

To decide in what order we will fix the issues reported, we look at the impact, severity and exploit complexity. Vulnerability reports might take some time to prioritize or fix. We need time to focus on the remediation, so you are welcome to ask about the status of your report, but we will aim to respond to you within 14 working days.

We will notify you when the vulnerability you reported is fixed, and we may ask you to confirm that the solution works. You are also welcome to tell others about your disclosure and the resolution (for example on a blog or your own website). You will need to tell us when you plan to publish this so we can make sure affected users have also received the guidance needed.

We welcome feedback on the disclosure handling process, the clarity and quality of the communication, and of course the effectiveness of the vulnerability resolution. This feedback will be used in strict confidence to help us improve our processes for handling reports, developing services, and resolving vulnerabilities.

6. Guidance

You must not:

- break any applicable law or regulations
- access unnecessary, excessive or significant amounts of data
    - for example, 2 or 3 records are enough to demonstrate most vulnerabilities such as enumeration or direct object reference vulnerability
- modify data in our systems or services that do not belong to the researcher
- use high-intensity invasive or destructive technical security scanning tools to find vulnerabilities
- attempt or report any form of denial of service, for example, overwhelming a service with a high volume of requests
- disrupt our 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 this policy or with anyone other than their assigned CCS security contact

- violate the privacy of qiio users, staff, contractors, services or systems
    - for example: by sharing, redistributing and/or not properly securing data retrieved from our systems or services
- social engineer, 'phish' or physically attack qiio staff or infrastructure
- demand financial compensation before disclosing any vulnerabilities

You must:

- always comply with data protection rules and must not violate the privacy of any data that qiio 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)

7. Legalities

This policy is designed to be compatible with common good practice among well-intentioned security researchers. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause qiio to be in breach of any of its legal obligations

We affirm that we will not seek prosecution of any security researcher who reports any security vulnerability on a qiio service or system, where the researcher has acted in good faith and in accordance with this disclosure policy.