Vulnerability Disclosure Policy
Groupe Equasens and subsidiaries

Document change history

Version	Date	Description
1.0	2023-06-01	First release

Introduction

This policy describes **what systems** and **types of research** are covered **under this policy**, how to send us **vulnerability reports**, and how long we ask security researchers to wait before **publicly disclosing** vulnerabilities.

We encourage you to contact us to report potential vulnerabilities in our systems.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized we will work with you to understand and resolve the issue quickly, and EQUASENS will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

EQUASENS makes no commitment that external parties will not take legal action against you.

In order to mitigate any related risk, we insist on the necessity to inform us about found vulnerabilities as soon as possible, and not to try to get deeper into the vulnerable system.

This policy only covers systems implemented and operated under the responsibility of EQUASENS. You are advised that these systems may be interconnected with systems of other organizations, which are not covered by this policy.

Guidelines

Under this policy, “research” means activities in which you:

- ✓ Notify us as soon as possible after you discover a real or potential security issue.
- ✓ Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- ✓ Only use exploits to the extent necessary to confirm a vulnerability’s presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- ✓ Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- ✓ Do not submit a high volume of low-quality reports.

Once you’ve established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

Test methods

The following test methods are not authorized:

- ✓ Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- ✓ Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

Scope

The policy covers web sites and web applications managed by and under the responsibility of EQUASENS.

The web sites and web applications of subsidiaries are included.

EQUASENS is registered with RIPE as ORG-PIS20-RIPE. This does not imply that all IP ressources registered in RIPE's registry under this handle are covered by the present policy.

Bug bounty program

EQUASENS has no bug bounty program yet.

Reporting a vulnerability

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities.

If your findings include newly discovered vulnerabilities that affect all users of a product or service of a third party, we may share your report with this third party, where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without express permission.

We accept vulnerability reports at :

csirt@equasens.com

If you share contact information, we will acknowledge receipt of your report within 3 business days.

If you want to submit sensitive data, we should encrypt it using this PGP key.

What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports:

- ✓ Describe the location the vulnerability was discovered and the potential impact of exploitation.
- ✓ Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- ✓ Be in English or French, if possible.

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- ✓ Within 3 business days, we will acknowledge that your report has been received.
- ✓ To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- ✓ We will maintain an open dialogue to discuss issues.

Questions

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