Security Disclosure Policy

At TWTG R&D B.V., we consider the security of our systems and the protection of our customer’s data a top priority.

We greatly appreciate investigative work into security vulnerabilities, which is carried out by well-intentioned, ethical security researchers. We are committed to thoroughly investigating and resolving security issues in our platform and services in collaboration with the wider security community. This document aims to define a method by which we can work with the security research community to improve our online security.

If a vulnerability was to be discovered, we would like to know about it so we can take the necessary steps to address it as quickly as possible. We would like to request any information that will support us better protect our processes and our systems.

Scope

- TWTG embedded products as mentioned on our Product page
- TWTG software products (e.g. SolidRed)
- TWTG online services (e.g. Service desk and Product documentation platform)

Reporting a vulnerability

- Email your findings to security.report (at) twtg (dot) io
- Provide sufficient information to reproduce the problem, so we will be able to resolve it in due course.

Guidance

Security researchers are expected to:

- Not take advantage of the vulnerability or problem discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data;
- Not reveal the problem to others until it has been resolved;
- Not arrange attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties;
- Not violate any laws or agreements to discover vulnerabilities;
- Not modify data in our systems/services.

We request that any and all data retrieved during research is securely deleted as soon as it is no longer required and at most, one month after the vulnerability is resolved, whichever occurs soonest.

If you are unsure at any stage whether the actions you are thinking of taking are acceptable, please contact our security team for guidance (please do not include any sensitive information in the initial communications): security (dot) report (at) twtg (dot) io.

What to expect

- We will respond to a report within 96 hours with an acknowledgment of receiving the vulnerability report and an expected resolution date
- Information will be shared, once the vulnerability is resolved

We would like to thank any researcher who submits a vulnerability report.
We strive to resolve all problems as quickly as possible.

Capelle aan den IJssel, 05-06-2023

Nadine Herrwerth
CEO