Coordinated Vulnerability Disclosure Policy

Solar Tıp Teknolojileri A.Ş. (SolarMedtec) · Coordinated vulnerability disclosure policy under Regulation (EU) 2024/2847, Annex I, Part II · SMQM23 Rev 00

1. Purpose

SolarMedtec welcomes reports of potential security vulnerabilities in its products. This policy explains how to report a vulnerability to us, how we handle a report once we have it, and what a reporter can expect from us in return. It is published so that anyone who finds a weakness in one of our products has a clear, predictable and safe route to tell us about it.

2. Scope

This policy covers:

- all instruments and other products with digital elements placed on the market by SolarMedtec, including instruments supplied to partners and sold under a partner's own brand;
- the firmware embedded in those instruments, together with the host software and the communication protocol we supply with them;
- the web pages we operate for product information and product support.

This policy does not cover:

- products of other manufacturers that are used alongside our instruments;
- third-party services, platforms or web sites that we do not operate;
- software written by a partner or a customer on top of our communication protocol, which should be reported to whoever wrote it.

Where an instrument is sold under a partner's brand, a reporter may use either this channel or the partner's channel. We coordinate with the partner in either case, and using this channel never costs a reporter time.

3. How to report

E-mail	security@galvanoplot.com
Encryption (optional)	Not currently provided
Web	https://galvanoplot.com/security
Language	English or Turkish
Anonymous reports	Accepted. We cannot send you status updates or credit you if you leave no contact address.

Please include, as far as it is available to you:

- the affected product and its firmware or software version;
- the serial number, where one applies;
- a description of the vulnerability and of its potential impact;
- the steps needed to reproduce it;
- any proof-of-concept code, configuration or capture that helps us reproduce it.

Please do not include personal data of third parties, patient data or customer data in your report. If a screenshot or a capture contains such data, redact it before sending.

4. What we ask of reporters

- Give us a reasonable opportunity to investigate and remediate before public disclosure. We propose a coordinated disclosure period of 90 days from our acknowledgement, and we will tell you promptly, with our reasons, if we need longer.
- Test only on equipment that belongs to you or that you are authorised to test.
- Do not access, modify or delete data that does not belong to you.
- Do not degrade the availability of any product or service, and do not run denial-of-service or load tests.
- Do not test instruments that are in clinical, diagnostic, production or other live use.
- Do not use social engineering, phishing or physical intrusion against our staff, our customers or our premises.
- Act in good faith and in accordance with applicable law.

5. Safe harbour

If you follow this policy, we will treat your research as authorised by us. We will not pursue or support legal action against you in relation to it, and we will not report you to a law enforcement authority for it. Should a third party bring an action against you for research carried out in accordance with this policy, we will state that your activity was authorised by us. This commitment does not extend to activity that goes beyond this policy, and it cannot bind a third party whose systems you may have touched.

6. Reports we normally do not act on

We read every report. The following, however, are normally closed without remediation unless a concrete impact is demonstrated: missing security headers or cookie flags with no working exploit; raw output of automated scanners without analysis; the presence of an outdated library with no exploitable path in our product; theoretical weaknesses with no practical attack; attacks that require physical disassembly of the instrument together with a level of access that no realistic user has; service degradation through excessive load; social engineering.

7. No bug bounty

We do not operate a paid bug bounty programme and we offer no monetary reward. What we do offer is public credit, on the terms set out below.

8. What we commit to

Step	Our commitment
Acknowledgement	Within 3 working days of receiving the report
Initial assessment	Within 10 working days: whether we could reproduce the issue, and an initial severity rating using CVSS
Status updates	At least every 30 days until the report is closed
Remediation	A correction, a mitigation, or a documented and explained decision to accept the risk, with a target date communicated to you
Advisory	A security advisory for any vulnerability that affects products already in use, published on our security page
Credit	Public acknowledgement under the name or handle you choose, unless you prefer to stay anonymous
Closure	A closing message that explains the outcome
Legal position	We will not pursue legal action against reporters who act in good faith and in accordance with this policy

9. How we handle a report

On arrival a report is entered in our vulnerability register, together with the date and the time at which we became aware of it. A named security contact acknowledges it, and a technical owner attempts to reproduce the issue and rates its severity. We then assess two questions in particular: whether the

vulnerability is being actively exploited, and whether an incident affecting the security of the product has occurred, because the answers determine our legal duties towards the authorities. A correction or mitigation is developed, verified and released; an advisory is issued where products already in use are affected; and the report is closed with a record of the decision taken and of any change we have made to our own practice as a result.

Every step is recorded with the person responsible and the date. A deputy is named for each role so that the clock described in the next section never depends on one person being available. Records are retained for at least ten years after the product concerned was last placed on the market, or for the duration of its support period, whichever is longer.

10. Reporting to the authorities

Where a vulnerability in one of our products with digital elements is actively exploited, or where a severe incident affecting the security of such a product occurs, Regulation (EU) 2024/2847 requires the manufacturer to notify, simultaneously, the computer security incident response team (CSIRT) designated as coordinator and the European Union Agency for Cybersecurity (ENISA):

Notification	Deadline
Early warning	Within 24 hours of becoming aware
Vulnerability or incident notification	Within 72 hours of becoming aware
Final report – actively exploited vulnerability	Within 14 days after a corrective or mitigating measure is available
Final report – severe incident	Within one month after the incident notification

A vulnerability that we find ourselves and correct, and that is not being exploited, does not trigger these notifications; it is handled through the process described above and, where users are affected, through an advisory.

We also inform affected users without undue delay and, where it is needed, tell them what they can do to reduce the risk in the meantime. Where an instrument is placed on the market under a partner's own brand, that partner is the manufacturer for the purpose of these obligations and makes the notification; we supply the partner with the technical information required, early enough for the partner to meet the deadlines above.

11. Security updates and the support period

Security updates are provided free of charge throughout the declared support period of the product.

Product	GX100 Series Super-Compact Potentiostats
Support period	5 years from the date the unit was placed on the market
Update route	Dedicated firmware updater application for Windows over USB
Integrity of an update	Verification of SHA256 hash of the firmware binary
Advisory	Published whenever an update addresses a vulnerability that affects products already in use

12. How we handle your personal data

If you give us a contact address, we use it only to correspond with you about your report and to credit you if you wish to be credited. Your report and our correspondence are kept as part of the vulnerability record. We do not disclose your identity to a third party without your consent, unless the law requires us to. You may ask us at any time to remove your contact details from our records.

13. Document control

Revision / date	00 / 07.10.2026
Owner	Software Quality Management
Approved by	Emre Kurtulan
Review interval	Annually, or upon regulatory or organisational change
Published at	https://galvanoplot.com/security