

SECURITY

Coordinated Vulnerability Disclosure Policy

How to report a security vulnerability in HARDWARIO products, services or websites, what we do with your report, and on what terms good-faith security research is welcome.

DOCUMENT: HLN.261009.01-R1 VALID FROM: October 9, 2026

1. Contact

E-mail	security@hardwario.com
Languages	English, Czech
Security advisories	https://www.hardwario.com/security/

This is our single point of contact for reporting vulnerabilities and for information about them. If e-mail does not suit you, write to ask@hardwario.com or to HARDWARIO a.s., U Jezu 525/4, 460 01 Liberec, Czech Republic, and we will agree on another way to communicate.

2. Scope

This policy covers HARDWARIO products with digital elements (devices and their firmware, for example CHESTER, STICKER, EMBER, FIBER and GAUGER), HARDWARIO Cloud and the HARDWARIO websites (www.hardwario.com, docs.hardwario.com and the other websites on HARDWARIO domains).

It does not cover systems that HARDWARIO does not own or operate: customers' installations and infrastructure, third-party services (for example the store platform, cloud and e-mail services) or devices that belong to someone else. We cannot authorise access to them. Please do report a vulnerability in a third-party component that our products use; we will pass it on to the component's maintainer.

3. How to report a vulnerability

Send us an e-mail that is as specific as possible:

- the affected product, service or website, and the firmware or software version,
- a description of the vulnerability and its possible impact,
- how to reproduce it (steps, proof-of-concept code, logs),
- whether you know of it being exploited,
- how we can reach you, and whether you wish to be credited in the advisory.

You may report anonymously. You may also report the vulnerability to the Czech National Cyber and Information Security Agency (NÚKIB), the Czech coordinator for coordinated vulnerability disclosure.

4. What we do with your report

- We confirm receipt within 3 working days.
- Within 10 working days we send you our first assessment: whether we confirm the vulnerability, how severe it is and what happens next.
- We keep you informed about the fix.
- We disclose the vulnerability in coordination with you, at the latest 90 days after your report; earlier once a fix is available, later only by agreement if the fix needs more time.
- Once it is fixed, we publish an advisory at <https://www.hardwario.com/security/>: the affected products and versions, a description and severity of the vulnerability, and how to remedy it. With your consent we credit you.
- We report actively exploited vulnerabilities and severe incidents as required by Regulation (EU) 2024/2847 through the ENISA single reporting platform to the coordinator, which for HARDWARIO is NÚKIB, and we inform the affected users.

5. Good-faith security research

We consider research within the scope of this policy, carried out in good faith and in line with it, to be authorised, and we will not take legal action against you for it. This policy is HARDWARIO's consent as the owner of the systems concerned; we cannot consent for systems owned by others.

Please:

- test only devices and accounts that you own or that their owner has allowed you to test,
- not access, change or delete other people's data beyond what is needed to demonstrate the vulnerability; if you come across personal data, stop, do not copy it and tell us,
- not disrupt our services (no denial-of-service attacks, flooding or spam) and not use social engineering or physical access,
- not disclose the vulnerability before we have fixed it or the period in Article 4 has passed,
- not demand anything in return for the report under the threat of disclosure.

6. Personal data

We process the personal data in a report (in particular your name and e-mail) to handle the report, as described in the HARDWARIO Privacy Notice.

7. Changes to this policy

Each version carries a document number, revision and valid-from date; all earlier versions are available at <https://www.hardwario.com/legal/>.