Product Security & Vulnerability Reporting

Sonifex takes the security of its products seriously and welcomes responsible reports of potential cybersecurity vulnerabilities.

If you believe you have identified a security vulnerability affecting a Sonifex product, please report it to:

security@sonifex.co.uk

This address is our primary contact point for product security and vulnerability reports.

What to include in your report

Please provide as much of the following information as possible:

- the Sonifex product model;
- firmware or software version, where known;
- a description of the suspected vulnerability;
- the steps required to reproduce the issue;
- details of the network or system configuration in which the issue was identified;
- the potential security impact;
- any proof-of-concept information, logs or screenshots that may assist our investigation;
- whether you are aware of the vulnerability being actively exploited.

Please do not include passwords, private keys, customer credentials or unnecessary personal information.

What happens after you report an issue?

Sonifex will review reports to determine whether the issue represents a genuine cybersecurity vulnerability and which products or firmware versions may be affected.

Where appropriate, we may contact you for additional technical information.

Confirmed vulnerabilities will be assessed and handled in accordance with our product security and vulnerability-management processes. This may include:

- further technical investigation;
- development and testing of a firmware or software update;
- identification of temporary mitigations;
- notification of affected users where appropriate;
- coordination with suppliers or maintainers of affected third-party components;
- statutory reporting to the appropriate cybersecurity authorities where required.

Not every software defect or unexpected product behaviour constitutes a cybersecurity vulnerability.

Coordinated vulnerability disclosure

We ask security researchers and other reporters to give Sonifex a reasonable opportunity to investigate and, where necessary, develop and distribute corrective measures before publishing detailed information that could enable exploitation of a vulnerability.

Where possible, please:

- avoid accessing, modifying or deleting data belonging to other users;
- avoid actions that could disrupt customer systems or services;
- limit testing to the minimum necessary to demonstrate the issue;
- do not use a vulnerability for commercial exploitation, extortion or unauthorised access;
- allow us reasonable time to investigate and respond before public disclosure.

We will aim to maintain communication with reporters while an issue is being investigated and will coordinate disclosure where appropriate.

Security updates

Where a security update or other corrective measure is required, Sonifex will provide information appropriate to the affected product and vulnerability.

Customers are encouraged to maintain products at an appropriate supported firmware/software version and to follow any security advisories or mitigation guidance issued by Sonifex.

Cyber Resilience Act

Sonifex products incorporating digital or network-connected functionality may fall within the scope of Regulation (EU) 2024/2847, the EU Cyber Resilience Act (CRA).

From **11 September 2026**, manufacturers are required to report certain cybersecurity events, including actively exploited vulnerabilities and severe security incidents affecting products with digital elements, through the applicable EU reporting process.

Where a vulnerability reported to Sonifex meets the relevant statutory reporting criteria, Sonifex will make the required notifications to the appropriate authorities.

The person reporting a vulnerability to Sonifex does not need to determine whether the issue is reportable under the Cyber Resilience Act. Sonifex will make that assessment as part of its investigation.

Contact

For product security and vulnerability reports:

security@sonifex.co.uk

For general product support, sales enquiries or other non-security matters, please use the normal contact details provided on the Sonifex website.