Vulnerability Disclosure Policy

Version: 1.0
Effective date: 2 November 2026

Purpose

Stresstech is committed to the security of our products and appreciates the efforts of customers, researchers, and other parties who responsibly identify and report potential security vulnerabilities.

This policy explains how to report a suspected vulnerability and how Stresstech will respond.

Reporting a Vulnerability

If you believe you have discovered a security vulnerability in a Stresstech product or software application, please report it on our website at www.stresstech.com. See the *Product Security* page for instructions.

Please include, where possible:

- Product name and model
- Software or firmware version
- Description of the vulnerability
- Steps to reproduce the issue
- Potential impact
- Any supporting files, screenshots, or proof-of-concept code

What You Can Expect

After receiving your report, we will:

- Acknowledge receipt within **5 business days**.
- Assess the reported vulnerability.
- Contact you if additional information is required.
- Keep you informed of significant progress where appropriate.
- Work to develop and distribute a fix when necessary.

Response times may vary depending on the complexity and severity of the issue.

Responsible Disclosure

We kindly request that you:

- Do not publicly disclose the vulnerability before we have had a reasonable opportunity to investigate and address it.
- Avoid actions that could harm our customers or services.
- Only access systems or data necessary to demonstrate vulnerability.
- Do not modify or destroy customer data.

Address
Stresstech Oy
Tikkutehtaantie 1
FIN-40800 VAAJAKOSKI
Finland

Invoicing address
Stresstech Oy
Sarjanr 16800633
PL 861
00019 SSC
Finland

Network Service ID
TE003720452813

Telephone
+358 14 333 000

VAT number
FI20452813

Email
info@stresstech.com

Web
www.stresstech.com

- Comply with all applicable laws.

Our Commitment

Stresstech values responsible security research and will:

- Review all reported vulnerabilities in good faith.
- Treat reports confidentially where appropriate.
- Coordinate disclosure with the reporter whenever practical.
- Credit the reporter in public advisories if they wish to be acknowledged.

Scope

This policy applies to:

- Stresstech hardware products with digital components
- Embedded firmware
- Application software

Standalone third-party products that are not supplied as part of a Stresstech product are outside scope. Vulnerabilities in third-party components embedded in, bundled with, or required by a Stresstech product should still be reported to Stresstech. We will coordinate with the relevant supplier where appropriate.

Security Advisories

Stresstech will publish or otherwise make available security information about:

- Affected products
- Severity
- Available mitigations
- Software or firmware updates
- Relevant CVE identifiers (if assigned)

Legal Notice

This policy does not authorize activities that violate applicable laws, regulations, or contractual obligations.