Master Therm tepelná čerpadla s.r.o.
Dolní Tříč 636, 512 43 Jablonec nad Jizerou, Czech Republic
ID No.: 28892275 · VAT: CZ28892275

Coordinated Vulnerability Disclosure (CVD) Policy

Published in accordance with Regulation (EU) 2024/2847 (Cyber Resilience Act) – point of contact for reporting vulnerabilities and security incidents

Master Therm tepelná čerpadla s.r.o. (“Master Therm”) welcomes the responsible reporting of security vulnerabilities in our products. This policy sets out the rules for reporting them safely and for their coordinated disclosure.

SCOPE

This policy applies to Master Therm software and online services related to the control, monitoring and remote management of Master Therm heat pumps, in particular:

- the embedded software and firmware of the heat pump's control system and control panel
- the web portals, their backend services and related APIs
- the user and service web application
- the MasterTherm mobile applications for iOS and Android
- the communication mechanisms between these system components and the mechanisms used to distribute their updates.

This policy does not apply to third-party devices, services and systems that are not under Master Therm's control.

If you discover a vulnerability in a third-party component that is part of our product, you may report it to us as well. Where necessary, we will coordinate its resolution with the manufacturer or administrator of the affected component.

HOW TO REPORT A VULNERABILITY

Please report the vulnerability to us at:

E-mail: security@mastertherm.cz
Please encrypt sensitive information with the **PGP key** published in our security.txt file:

security.txt: https://www.mastertherm.cz/.well-known/security.txt

We accept reports in Czech and English.

If possible, please include:

- the affected product and its version
- whether the issue concerns the control panel, the web, service or mobile application, the backend/API, or another interface
- a description of the vulnerability and its potential impact
- steps allowing us to reproduce the issue
- proof of concept, logs or other technical information, where available

- whether the issue was verified on your own device or account
- whether, to your knowledge, the vulnerability is being actively exploited.

Please do not include personal data, login credentials or other users' data unless necessary to substantiate the issue. We recommend sending sensitive information in encrypted form.

If you are not sure whether an issue you found constitutes a security vulnerability, you may still report it. We will assess it.

OUR COMMITMENT

We will endeavor to:

- acknowledge receipt of your report within 3 business days
- share the outcome of our initial assessment within 10 business days
- provide reasonable status updates if resolution takes longer
- analyze the vulnerability and take appropriate corrective or mitigating measures
- coordinate disclosure of the vulnerability with the finder, taking into account its severity and the complexity of the fix.

The time required to remediate a vulnerability depends on its nature, severity and the products affected.

We will treat reports as confidential. We will not disclose the finder's identity without their consent, except where required to do so by law or by a competent authority.

SAFE HARBOR

We will not pursue legal action against finders who conduct security research **in good faith and within the bounds of this policy** solely because of that research.

While conducting research, please refrain in particular from:

- accessing accounts, heat pumps or data belonging to other users beyond what is necessary to demonstrate the vulnerability
- changing the settings or operation of another person's heat pump
- any action that could cause unsafe operation, damage to equipment, or a significant change in conditions at the premises
- intentionally disrupting the availability of services or equipment
- deleting or modifying other people's data
- social engineering of employees, service partners, installation companies, customers or other persons
- installing malicious software
- continuing to probe a system after the vulnerability has been sufficiently demonstrated
- demanding a reward or other benefit under threat of disclosing the vulnerability.

Please conduct testing primarily on a device and account that you own or are authorized to test.

If, during your research, you unintentionally gain access to another person's device, account, or to non-public or personal data, do not make further use of that access and limit any processing of the information obtained to the minimum necessary to report the vulnerability.

Safe harbor applies only to products, services and systems that Master Therm is authorized to consent to being tested. It cannot create authorization to test third-party systems, nor does it limit their rights or the powers of public authorities.

If you are unsure whether a particular testing method complies with this policy, please contact us before carrying it out at **security@mastertherm.cz**.

COORDINATED DISCLOSURE

We ask finders to give us reasonable time to analyze and remediate a vulnerability, and to coordinate disclosure of technical details with us before publishing them.

Once a security update or other corrective measure is available, we may publish a security advisory containing, in particular, information about the affected product and versions, a description and severity rating of the vulnerability, and instructions for remediation or updating.

ACKNOWLEDGEMENTS AND REWARDS

With the finder's consent, we may credit their name or pseudonym in the acknowledgements of the relevant security advisory.

This policy is not a bug bounty program, and reporting a vulnerability does not automatically entitle the finder to a financial or other reward.

Effective date: 11 September 2026
Version: 1.0
Contact: **security@mastertherm.cz**