Master Therm tepelná čerpadla s.r.o.
Dolní Tříč 636, 512 43 Jablonec nad Jizerou, ČR
IČO: 28892275 · DIČ: CZ28892275

Politika koordinovaného zveřejňování zranitelností (CVD)

Zveřejněno v souladu s nařízením (EU) 2024/2847 (Cyber Resilience Act) – kontaktní místo pro hlášení zranitelností a bezpečnostních incidentů

Společnost **Master Therm tepelná čerpadla s.r.o.** („Master Therm“) vítá odpovědné hlášení bezpečnostních zranitelností v našich produktech. Tato politika stanoví pravidla pro jejich bezpečné oznámení a koordinované zveřejnění.

ROZSAH

Tato politika se vztahuje na software a online služby Master Therm související s ovládáním, monitoringem a vzdálenou správou tepelných čerpadel Master Therm, zejména na:

- embedded software a firmware řídicího systému a ovládacího panelu tepelného čerpadla
- webové portály, jejich backendové služby a související API
- uživatelskou a servisní webovou aplikaci
- mobilní aplikace MasterTherm pro iOS a Android
- mechanismy komunikace mezi těmito částmi systému a mechanismy distribuce jejich aktualizací.

Politika se nevztahuje na zařízení, služby a systémy třetích stran, které nejsou pod kontrolou Master Therm.

Pokud zjistíte zranitelnost komponenty třetí strany, která je součástí našeho produktu, můžete ji oznámit také nám. Podle potřeby budeme její řešení koordinovat s výrobcem nebo správcem dotčené komponenty.

JAK ZRANITELNOST NAHLÁSIT

Zranitelnost nám prosím oznamte na:

E-mail: security@mastertherm.cz
Citlivé informace šifrujte klíčem PGP zveřejněným v souboru security.txt:

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

Přijímáme hlášení v českém a anglickém jazyce.

Pokud je to možné, uveďte:

- dotčený produkt a jeho verzi
- zda se problém týká ovládacího panelu, webové, servisní nebo mobilní aplikace, backendu/API nebo jiného rozhraní
- popis zranitelnosti a jejího možného dopadu
- postup umožňující problém reprodukovat
- případně proof of concept, logy nebo jiné technické informace

- zda byl problém ověřen na vašem vlastním zařízení nebo účtu
- zda podle vašich poznatků dochází ke skutečnému zneužívání zranitelnosti.

Nepřikládejte osobní údaje, přihlašovací údaje nebo data jiných uživatelů, nejsou-li nezbytná k doložení problému. Citlivé informace doporučujeme zasílat šifrovaně.

Pokud si nejste jisti, zda nalezený problém představuje bezpečnostní zranitelnost, můžete jej přesto oznámit. Posoudíme jej.

NÁŠ ZÁVAZEK

Budeme usilovat o to, abychom:

- potvrdili přijetí hlášení do 3 pracovních dnů
- sdělili výsledek prvotního posouzení do 10 pracovních dnů
- při delším řešení poskytovali přiměřené informace o jeho průběhu
- zranitelnost analyzovali a přijali přiměřená nápravná nebo zmírňující opatření
- zveřejnění zranitelnosti koordinovali s nálezcem s ohledem na její závažnost a složitost nápravy.

Doba potřebná k odstranění zranitelnosti závisí na její povaze, závažnosti a dotčených produktech.

S hlášením budeme nakládat důvěrně. Identitu nálezce bez jeho souhlasu nezveřejníme, s výjimkou případů, kdy nám takovou povinnost ukládá právní předpis nebo příslušný orgán.

BEZPEČNÝ PŘÍSTAV

Proti nálezcům, kteří při bezpečnostním výzkumu jednají **v dobré víře a v mezích této politiky**, nebudeme z důvodu takového výzkumu podnikat právní kroky.

Při výzkumu se zdržte zejména:

- přístupu k účtům, tepelným čerpadlům nebo datům jiných uživatelů nad rozsah nezbytný k prokázání zranitelnosti
- změny nastavení nebo ovládání tepelného čerpadla jiné osoby
- jednání, které může způsobit nebezpečný provoz, poškození zařízení nebo významnou změnu podmínek v objektu
- úmyslného narušování dostupnosti služeb nebo zařízení
- mazání nebo změny dat jiných osob
- sociálního inženýrství zaměstnanců, servisních partnerů, instalačních firem, zákazníků nebo jiných osob
- instalace škodlivého softwaru
- pokračování v průniku poté, co byla zranitelnost dostatečně prokázána
- požadování odměny nebo jiné výhody pod pohrůžkou zveřejnění zranitelnosti.

Testování provádějte přednostně na zařízení a účtu, které vlastníte nebo k jejichž testování máte oprávnění.

Pokud při výzkumu neúmyslně získáte přístup k zařízení, účtu nebo neveřejným či osobním údajům jiné osoby, dále tento přístup nevyužívejte a omezte zpracování získaných informací na minimum nezbytné k oznámení zranitelnosti.

Bezpečný přístav se vztahuje pouze na produkty, služby a systémy, k jejichž testování je Master Therm oprávněn dát souhlas. Nemůže založit oprávnění k testování systémů třetích stran ani omezit jejich práva nebo pravomoci orgánů veřejné moci.

Máte-li pochybnosti, zda je určitý způsob testování v souladu s touto politikou, kontaktujte nás před jeho provedením na **security@mastertherm.cz**.

KOORDINOVANÉ ZVEŘEJNĚNÍ

Žádáme nálezce, aby nám poskytli přiměřený čas k analýze a nápravě zranitelnosti a před zveřejněním technických detailů s námi zveřejnění koordinovali.

Jakmile je k dispozici bezpečnostní aktualizace nebo jiné nápravné opatření, můžeme zveřejnit bezpečnostní oznámení obsahující zejména informace o dotčeném produktu a verzích, popis a závažnost zranitelnosti a pokyny k nápravě nebo aktualizaci.

PODĚKOVÁNÍ A ODMĚNY

Se souhlasem nálezce můžeme uvést jeho jméno nebo pseudonym v poděkování u příslušného bezpečnostního oznámení.

Tato politika není bug bounty programem a za oznámení zranitelnosti nevzniká automatický nárok na finanční nebo jinou odměnu.

Účinnost: 11. září 2026
Verze: 1.0
Kontakt: **security@mastertherm.cz**