Vulnerability Disclosure Policy and Defined Support Period

Introduction

Kohler Mira Ltd. is committed to safeguarding and protecting our information and any other information entrusted to us by our customers through use of our website, connected products or any other medium of transmission over the internet.

We take cyber-security and privacy issues seriously and recognise the trust placed in us as manufacturers to handle customer data with the utmost importance and the need to ensure that data is secure. As such, we are committed to addressing and reporting security issues through a coordinated and constructive approach; designed to drive the greatest protection for technology users and protection of Kohler Mira Ltd. information along with information relating to our customers, consumers and employees.

This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy also describes what systems and types of research are covered under this policy, how to send us vulnerability reports, and how long we ask security researchers to wait before publicly disclosing vulnerabilities.

We encourage you to contact us to report potential vulnerabilities in our systems.

Defined Support Period for Connected Products

Kohler Mira Ltd. shall endeavour to continue support of our Internet connected products for as long as practicable after the formal notification of obsolescence of a product line. Customers can expect to continue to be supported with the following for a minimum period of 5 years after product withdrawal from the market.

- Functional bug fixes in product firmware/software.
- Security critical firmware/software updates.
- Mobile app updates that interact with our internet connected products to provide additional functionality.

Mobile app updates will be maintained for the current version and up to 2 previous major version releases for both iOS and Android platforms.

Reporting security issues

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorised, we will work with you to understand and resolve the issue quickly, and Kohler Mira Ltd. will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorisation known.

When properly notified of legitimate issues, we will do our best to acknowledge your vulnerability report, assign resources to investigate the issue, and fix potential problems as quickly as possible. Whether you are a user of Kohler Mira Ltd. products, a software developer, or simply a security enthusiast, you are an important part of this process.

If you believe you have discovered a vulnerability in a Kohler Mira Ltd. asset / system or have a security incident to report, please send an email to KohlerGlobalDataPrivacy@kohler.com with as much details as possible.

In all cases, you must:

- Respect our privacy
  - Contact us immediately if you access anyone else's data, personal or otherwise. This includes usernames, passwords and other credentials. You must not save, store or transmit this information.
- Act in good faith
  - You should report the vulnerability to us with no conditions attached.
- Work with us
  - Promptly report any findings to us, stopping after you find the first vulnerability and requesting permission to continue testing.
  - Allow us a reasonable amount of time to resolve the vulnerability before publicly disclosing it.

And you must not:

- Exfiltrate data. Instead use a proof of concept to demonstrate a vulnerability.
- Exploit a vulnerability to disable further security controls.
- Perform social engineering.
- Use automated scanners.

Guidelines
Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- Do not submit a high volume of low-quality reports.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

Test methods
The following test methods are not authorised:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.

- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.

Scope
This policy applies to the following systems and services:

- www.mirashowers.com
- www.kohler.com
- www.kohlermira.co.uk
- Kohler Mira Smart / Connected products

Any service not expressly listed above, are excluded from scope and are not authorised for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us at KohlerGlobalDataPrivacy@kohler.com before starting your research.

Though we develop and maintain other internet-accessible systems or services, we ask that active research and testing only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that you think merits testing, please contact us to discuss it first. We will increase the scope of this policy over time.

Reporting a vulnerability
We accept vulnerability reports via KohlerGlobalDataPrivacy@kohler.com. Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 3 business days.

We do not support PGP-encrypted emails. For particularly sensitive information, please get in contact initially at the address above and we can arrange for a secure method of communication.

By submitting a vulnerability, you acknowledge that you have no expectation of payment and that you expressly waive any future pay claims against Kohler Mira Ltd. related to your submission.

What we would like to see from you
In order to help us triage and prioritise submissions, we recommend that your reports:

- Describe the location the vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Be in English, if possible.

What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within 3 business days, we will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

Questions

Questions regarding this policy may be sent to KohlerGlobalDataPrivacy@kohler.com.

We also invite you to contact us with suggestions for improving this policy.