Responsible Disclosure Policy

Responsible Disclosure Policy

Purpose

To allow for the reporting and disclosure of vulnerabilities discovered by external entities, and anonymous reporting of information security policy violations by internal entities.

Scope

MotorK's Responsible Disclosure Policy applies to MotorK's core platform and its information security infrastructure, and to internal and external employees or third parties.

Background

MotorK is committed to ensuring the safety and security of our customers and employees. We aim to foster an environment of trust, and an open partnership with the security community, and we recognize the importance of vulnerability disclosures and whistleblowers in continuing to ensure safety and security for all of our customers, employees and company. We have developed this policy to both reflect our corporate values and to uphold our legal responsibility to good-faith security researchers that are providing us with their expertise and whistleblowers who add an extra layer of security to our infrastructure.

Roles and Responsibilities

IT Manager: Ensure that the Responsible Disclosure Policy remains relevant and up-to-date. Engage with other teams (like HR, Legal and PR) for comprehensive policy review.
HR: validate relevant contents of this policy related to employees
Legal: validate relevant contents of this policy that are related to Legal aspects
Chief R&D Officer: Approve major changes to the policy.

Legal Posture

MotorK will not engage in legal action against individuals who submit vulnerability reports through our Vulnerability Reporting inbox. We openly accept reports for the currently listed MotorK products. We agree not to pursue legal action against individuals who:

- Engage in testing of systems/research without harming MotorK or its customers.
- Engage in vulnerability testing within the scope of our vulnerability disclosure program.
- Test on products without affecting customers, or receive permission/consent from customers before engaging in vulnerability testing against their devices/software, etc.
- Adhere to the laws of their location and the location of MotorK. For example, violating laws that would only result in a claim by MotorK (and not a criminal claim) may be acceptable as MotorK is authorizing the activity (reverse engineering or circumventing protective measures) to improve its system.
- Refrain from disclosing vulnerability details to the public before a mutually agreed-upon timeframe expires.

Policy

Vulnerability Report/Disclosure

How to Submit a Vulnerability

To submit a vulnerability report to MotorK's Product Security Team, please utilize the following email **team.sec@motork.io.**

Preference, Prioritization, and Acceptance Criteria

We will use the criteria from the next sections to prioritize and triage submissions.

What we would like to see from you:

- Well-written reports in English will have a higher probability of resolution.
- Reports that include proof-of-concept code equip us to better triage.
- Reports that include only crash dumps or other automated tool output may receive lower priority.
- Reports that include products not on the initial scope list may receive lower priority.
- Please include how you found the bug, the impact, and any potential remediation.
- Please include any plans or intentions for public disclosure.

What you as a Customer can expect from MotorK:

- A timely response to your email (within 5 business days).
- After triage, we will send an expected timeline, and commit to being as transparent as possible about the remediation timeline as well as on issues or challenges that may extend it.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.

If we are unable to resolve communication issues or other problems, MotorK may bring in a neutral third party to assist in determining how best to handle the vulnerability.

Vulnerabilities that reveal an occurred or potential Data Breach

Should the vulnerability disclosed be considered also a sign of a potential or occurred data breach (which means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed) the internal Data Breach Management procedure will be activated.

Whistle Blowing

How to Submit a Report

To anonymously report an information security program violation or a violation of related laws and regulations, please refer to the Whistle Blowing policy of MotorK available at this link:

https://s29.q4cdn.com/307181961/files/doc_downloads/governance/2022/01/MotorK-plc-whistleblowing-policy-(rev2022.pdf

Version	Date	Editor	Approver	Description of Changes	Format
V1.1	2024-07-18	Enrico La Cava	Yair Pinyan	Policy review - no changes	Digital
V1	2023-07-18	Marco Sandrini	Yair Pinyan		Digital