Responsible disclosure policy

MotorK

Scopo

Consentire la segnalazione e la rivelazione di vulnerabilità scoperte da entità esterne e la segnalazione anonima di violazioni delle policy di sicurezza delle informazioni da parte di soggetti interni.

Ambito di applicazione

La Responsible Disclosure Policy di MotorK si applica alla piattaforma principale di MotorK e alla sua infrastruttura di sicurezza delle informazioni, nonché ai dipendenti interni ed esterni o a terzi.

Contesto

MotorK si impegna a garantire la sicurezza dei propri clienti e dipendenti, con l'obiettivo di promuovere un ambiente di fiducia e di collaborazione aperta con la comunità della sicurezza, riconoscendo l'importanza della divulgazione delle vulnerabilità e degli informatori per continuare a garantire la sicurezza di tutti i clienti, dei dipendenti e dell'azienda stessa.
Abbiamo sviluppato questa policy sia per riflettere i nostri valori aziendali sia per sostenere la nostra precisa responsabilità nei confronti dei collaboratori che in buona fede mettono a disposizione la loro esperienza sia degli informatori che contribuiscono ad aggiungere un ulteriore livello di sicurezza alla nostra infrastruttura.

Ruoli e responsabilità

Responsabile IT: Garantisce che la Responsible Disclosure Policy rimanga pertinente e aggiornata. Collabora con altri team (come HR, Legal e PR) per una revisione completa della policy.
Responsabile R&D: Approva le principali modifiche alla policy.

Esclusione di azioni legali

MotorK non intraprenderà azioni legali contro le persone che inviano segnalazioni di vulnerabilità attraverso la nostra apposita casella di posta elettronica dedicata alle segnalazioni. MotorK accetta apertamente segnalazioni per i prodotti MotorK e accetta di non intraprendere azioni legali contro

individui che:

- Eseguono test di sistemi/ricerca senza danneggiare MotorK o i suoi clienti
- Eseguono test di vulnerabilità nell'ambito del nostro programma di divulgazione delle vulnerabilità.
- Eseguono test sui prodotti senza influenzare i clienti o ricevere il permesso/consenso dai clienti prima di eseguire test di vulnerabilità sui loro dispositivi/software, ecc.
- Rispettano le leggi della propria giurisdizione o di quella di MotorK. Ad esempio, la violazione di leggi che comporterebbero solo un'azione civile da parte di MotorK (salvo non giustifichino un'azione penale) può essere accettabile in quanto MotorK ne sta implicitamente autorizzando tali attività (reverse engineering o elusione delle misure di protezione) al fine di migliorare il proprio sistema.
- Si astengono dal divulgare pubblicamente i dettagli della vulnerabilità prima di una data stabilita di comune accordo.

Policy

Rapporto di vulnerabilità/divulgazione

Come inviare una segnalazione di vulnerabilità

Per inviare una segnalazione di vulnerabilità al Product Security Team di MotorK utilizzare il seguente indirizzo e-mail:

team.sec@motork.io.

Preferenza, priorità e criteri di accettazione

MotorK utilizza i criteri definiti nelle seguenti sezioni per definire le priorità e il triage delle segnalazioni:

• Segnalazioni ben scritte e dettagliate avranno una maggiore probabilità di essere risolte;
• Segnalazioni che includono il codice proof-of-concept ci permettono di migliorare il triage;
• Segnalazioni che includono solo crash dump o altri risultati di strumenti automatici potrebbero ricevere una priorità inferiore;
• Le segnalazioni che includono prodotti non presenti nell'elenco iniziale possono ricevere una priorità inferiore.
• Includere le modalità di individuazione del bug, l'impatto e qualsiasi potenziale rimedio. • Includere eventuali piani o intenzioni di divulgazione al pubblico.

Cosa aspettarsi da MotorK:

• Una risposta tempestiva all'e-mail di segnalazione (entro 5 giorni lavorativi):
• Dopo il triage, MotorK condividerà la tempistica di risoluzione prevista e si impegnerà a essere il più trasparente possibile sulla tempistica di correzione e sui problemi o le sfide che potrebbero prolungarla;
• Un dialogo aperto per discutere i problemi;
• Notifica del completamento di ogni fase dell'analisi di vulnerabilità;

- Credito dopo che la vulnerabilità è stata convalidata e risolta;

In caso di problemi di comunicazione o di altra natura, MotorK potrebbe rivolgersi a una terza parte per determinare la miglior modalità di gestione della vulnerabilità.

Segnalazione di irregolarità (Whistleblowing)

Come inviare una segnalazione

Per segnalare in forma anonima una violazione del programma di sicurezza delle informazioni o una violazione delle leggi e dei regolamenti in materia, consultare la *Whistleblowing Policy* di MotorK disponibile al seguente link:

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

Storia della revisione

Versione	Data	Autore	Approvatore	Descrizione della modifica	Formato
V2	23/07/2024	Federica Arcoraci	Enrico La Cava	Traduzione	Digitale
V1	18/07/2023	Marco Sandrini	Yair Pinyan	-	Digitale