Il presente documento è una traduzione della seguente versione inglese [https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/. La versione tradotta è riportata solo per agevolare la consultazione e per comodità dell'utente. In caso di discrepanze o ambiguità, la versione inglese prevarrà e avrà la precedenza in ogni caso.

# DOCUMENTO DI SINTESI

***Esame preliminare post-incidente di CrowdStrike (Preliminary Post Incident Review o PIR): aggiornamento della Content Configuration che ha interessato il sensore Falcon e il sistema operativo Windows (BSOD)***

## Panoramica

Per restare al passo con l'evoluzione continua delle minacce informatiche, i prodotti di sicurezza forniscono regolarmente aggiornamenti dei propri contenuti. Tali aggiornamenti possono includere la raccolta di dati di telemetria, nuovi modelli di rilevamento delle minacce, rilevamenti di vulnerabilità e altri miglioramenti fondamentali. Grazie alla regolarità degli aggiornamenti, i prodotti di sicurezza possono adattarsi rapidamente alle minacce emergenti, garantendo una solida protezione degli utenti e dei loro sistemi.

## Cosa è successo: panoramica dell'incidente

Il 19 luglio 2024, alle 04:09 UTC, è stato rilasciato un aggiornamento delle configurazioni della componente di Rapid Response Content per il sensore Falcon sugli host Windows che eseguono il sensore nella versione 7.11 e versioni successive. Questo aggiornamento doveva raccogliere dati telemetrici sulle nuove tecniche di minaccia osservate da CrowdStrike, ma ha innescato degli arresti anomali (BSOD) sui sistemi che erano online tra le 04:09 e le 05:27 UTC. Gli host Mac e Linux non sono stati coinvolti. Gli host Windows che non erano online o che non si sono connessi durante l'arco di tempo interessato non sono stati impattati.

## Perché è successo: la causa dell'incidente

Gli arresti anomali sono stati causati da un malfunzionamento della componente di Rapid Response Content, che non è stato rilevato durante i controlli di validazione. Quando questi contenuti sono stati caricati dal sensore Falcon, hanno provocato una lettura della memoria fuori dai limiti, determinando un arresto anomalo di Windows (BSOD).

## Cosa sta facendo CrowdStrike per evitare che ciò si ripeta?

**Procedure di test del software avanzate**

- Miglioreremo i test dei Rapid Response Content con test di sviluppatori locali, di aggiornamento e ripristino dei contenuti, di stabilità e dell'interfaccia dei contenuti, nonché stress test, fuzzing e fault injection.
- Aggiungeremo ulteriori controlli di validazione al Content Validator per prevenire problematiche di questo tipo in futuro.

**Maggiore resilienza e capacità di ripristino**

- Rafforzeremo i meccanismi di gestione degli errori nel sensore Falcon per garantire che gli errori derivanti da contenuti problematici siano gestiti in modo efficiente.

**Strategia di utilizzo ottimizzata**

- Adotteremo una strategia di utilizzo scaglionata, partendo da un cd. deployment canary in un piccolo sottoinsieme di sistemi per poi passare gradualmente a una distribuzione più estesa.
- Miglioreremo il monitoraggio delle prestazioni del sensore e del sistema durante l'utilizzo scaglionato dei contenuti per individuare e mitigare tempestivamente eventuali problemi.
- Offriremo ai clienti maggiore controllo sulla distribuzione degli aggiornamenti dei Rapid Response Content, consentendo una selezione granulare di dove e quando gli aggiornamenti di configurazione vengono implementati.
- Forniremo notifiche sull'aggiornamento dei contenuti e sulle relative tempistiche.

**Convalida da parte di terzi**

- Effettueremo più revisioni dei codici di sicurezza con terze parti indipendenti.
- Eseguiremo revisioni indipendenti dei processi di qualità end-to-end, dallo sviluppo all'utilizzo.