Ce document est une traduction de la version anglaise suivante [https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/. Cette traduction est uniquement fournie afin d'en faciliter la compréhension. En cas de conflit ou d'ambiguïté, la version anglaise prévaudra toujours.

RÉSUMÉ

Rapport préliminaire après incident (PIR) CrowdStrike : mise à jour de la configuration du contenu ayant un impact sur l'agent Falcon et le système d'exploitation Windows (BSOD)

Présentation

Pour garder une longueur d'avance sur les cybermenaces, nouvelles ou en évolution, le contenu des produits de sécurité est mis à jour régulièrement. Ces mises à jour (aussi nommées Rapid Response Content) peuvent inclure de la collecte de données de télémétrie, de nouveaux modèles de détection des cybermenaces, de la détection des vulnérabilités ou d'autres améliorations cruciales. Grâce à ces mises à jour régulières, les produits de sécurité s'adaptent rapidement pour faire face aux cybermenaces émergentes et garantissent une protection robuste aux utilisateurs, ainsi qu'à leurs systèmes.

Ce qui s'est passé : aperçu de l'incident

Le 19 juillet 2024, à 04h09 UTC, une mise à jour de type Rapid Response Content de l'agent Falcon a été publiée pour les hôtes Windows exécutant la version 7.11 et les versions ultérieures. Conçue pour recueillir des données de télémétrie sur les nouvelles cybermenaces observées par CrowdStrike, cette mise à jour a provoqué une panne (BSOD) des systèmes qui étaient en ligne entre 04h09 et 05h27 UTC. Les hôtes Mac et Linux n'ont pas été affectés. Les hôtes Windows hors ligne ou non connectés pendant cette période n'ont pas été affectés.

Pourquoi c'est arrivé : cause de l'incident

Les pannes étaient dues à un défaut logiciel du Rapid Response Content qui n'a pas été détecté durant la phase de validation. Une fois chargé par l'agent Falcon, le contenu a entraîné un débordement de lecture de l'espace mémoire, provoquant une panne des systèmes Windows (BSOD).

Que fait CrowdStrike pour éviter que cela ne se reproduise ?

Procédure de test logiciel améliorée

- Améliorer le processus de test des mises à jour Rapid Response Content grâce aux types de tests suivants : tests locaux menés par les développeurs, tests de mise à jour du contenu et de restauration, tests de résistance, fuzzing, injection d'erreurs, tests de stabilité et test de l'interface de contenu.
- Ajouter des contrôles et vérifications supplémentaires dans le Content Validator pour éviter la survenue de problèmes similaires.

Résilience et capacité de récupération améliorées

- Renforcer les mécanismes de gestion des erreurs de l'agent Falcon pour garantir que les erreurs liées aux contenus problématiques sont gérées sans heurts.

Stratégie de déploiement affinée

- Adopter une stratégie de déploiement échelonné : commencer par un déploiement Canary sur un petit sous-ensemble de systèmes avant un déploiement à plus grande échelle.
- Améliorer la surveillance des performances de l'agent et du système pendant le déploiement échelonné du contenu, afin d'identifier et de corriger rapidement les problèmes.
- Offrir au client un meilleur contrôle sur le déploiement des mises à jour du Rapid Response Content, en permettant une sélection granulaire du moment et de l'endroit où ces mises à jour sont déployées.
- Envoyer des notifications de mise à jour du contenu et des créneaux prévus pour celle-ci.

Validation indépendante

- Assurer plusieurs révisions du code de sécurité par des tiers indépendants.
- Assurer des contrôles qualité indépendants de bout en bout, du développement au déploiement.