Este documento é uma tradução da seguinte versão em inglês: https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/. A versão traduzida é fornecida apenas para fins de referência e praticidade. Em caso de qualquer conflito ou ambiguidade, a versão em inglês sempre prevalecerá e terá precedência.

RESUMO EXECUTIVO

Revisão Pós-Incidente (RPI) Preliminar da CrowdStrike: Atualização da Configuração de Conteúdo com Impacto no Sensor Falcon e no Sistema Operacional Windows (BSOD)

Visão geral

Para ficar à frente das novidades e das ciberameaças em evolução contínua, os produtos de segurança passam rotineiramente por atualizações de conteúdo. Essas atualizações podem incluir coleta de telemetria, novos padrões de detecção de ameaças, detecção de vulnerabilidades e outros aprimoramentos cruciais. Com atualizações regulares, os produtos de segurança podem se adaptar rapidamente às ameaças emergentes, garantindo uma proteção robusta para usuários e seus sistemas.

O que aconteceu: visão geral do incidente

Em 19 de julho de 2024, às 04:09 UTC, uma atualização do Conteúdo de Resposta Rápida para o sensor Falcon foi publicada para hosts Windows executando a versão 7.11 e superior do sensor. O objetivo da atualização era coletar telemetria de novas técnicas de ameaça observadas pela CrowdStrike, mas acionou falhas (BSOD) em sistemas que estavam online entre 04:09 e 05:27 UTC. Os hosts Mac e Linux não foram afetados. Os hosts Windows que não estavam online ou que não se conectaram durante o referido período não foram afetados.

Por que aconteceu: causa do incidente

As falhas ocorreram devido a um defeito no Conteúdo de Resposta Rápida, que não foi detectado durante as verificações de validação. Quando o conteúdo foi carregado pelo sensor Falcon, ocorreu uma leitura de memória fora dos limites, levando a falhas no Windows (BSOD).

O que a CrowdStrike está fazendo para evitar que isso aconteça novamente?

Procedimentos de Teste de Software Aprimorados

- Aprimoramento dos testes do Conteúdo de Resposta Rápida usando tipos de teste como: testes locais por desenvolvedores, atualização e reversão de conteúdo, estresse, fuzzing, injeção de falhas, estabilidade e interface de conteúdo.
- Inclusão de verificações de validação adicionais no Validador de Conteúdo para evitar problemas semelhantes

Resiliência e Capacidade de Recuperação Aprimoradas

- Fortalecimento dos mecanismos de tratamento de erros no sensor Falcon para garantir que os erros de conteúdo problemático sejam gerenciados de maneira adequada.

Estratégia de Implementação Refinada

- Adoção de uma estratégia de implementação escalonada, começando com uma implementação parcial em um pequeno subconjunto de sistemas antes de uma implementação completa em etapas.
- Melhoria no monitoramento do desempenho do sensor e do sistema durante a implementação escalonada de conteúdo para identificar e atenuar os problemas imediatamente.
- Fornecimento de maior controle sobre a disponibilização das atualizações do Conteúdo de Resposta Rápida aos clientes, permitindo a seleção granular de quando e onde essas atualizações serão implementadas.
- Fornecimento de notificações sobre atualização de conteúdo e horários.

Validações por Terceiros

- Realização de várias análises independentes de códigos de segurança por meio de terceiros.
- Realização de análises independentes do processo de qualidade de ponta a ponta, desde o desenvolvimento até a implementação.