Falha do conector de crowdstrike kibana expõe credenciais confidenciais

Data: 2025-10-07 12:25:45

Autor: Inteligência Against Invaders

Uma questão de segurança no conector de crowdstrike de Kibana permite que os invasores

acessem credenciais de crowdstrike armazenadas.

A falha afeta várias versões de Kibana e pode expor credenciais nos espaços dentro da mesma implantação. A Elastic lançou atualizações para resolver esse problema e exorta os usuários a atualizar imediatamente.

Detalhes da vulnerabilidade

A falha, rastreada como CVE-2025-37728, surge da proteção insuficiente de credenciais no conector de crowdstrike.

Quando um conector é criado em um espaço de trabalho ou espaço dentro de Kibana, as credenciais usadas para acessar a API de crowdstrike são armazenadas em cache.

Cve id	Versões afetadas	Impacto	CVSS 3.1 Pontuação
CVE-2025-37728	7.x: ? 7,17.29 8.x: 8.14.0 a 8.18.7 8.19.x: 8.19.0 a 8.19.4 9.0.x: 9.0.0 a 9.0.7 9.1.x: 9.1.0 a 9.1.4	Vazamento de credencial parcial	5.4

Um usuário malicioso com acesso a outro espaço pode explorar esse mecanismo de cache para recuperar credenciais que pertencem a um espaço diferente.

A questão afeta qualquer instância de Kibana usando o Crowdstrike Conector e pode levar à divulgação não autorizada de credenciais.

Versões e impacto afetados

A vulnerabilidade afeta todas as versões não suportadas e suportadas do Kibana, que incluem o conector de crowdstrike antes dos lançamentos remendados.

Embora nenhuma modificação ou exclusão direta de dados seja possível através dessa falha, as credenciais vazadas podem permitir que os invasores consultem APIs de crowdstrike, colete dados de ameaças e potencialmente manipulem fluxos de trabalho de caça de ameaças.

O risco é classificado como média com uma pontuação CVSSV3.1 de 5,4, indicando que a exploração bem -sucedida requer privilégios limitados e alguma interação do usuário, mas pode

resultar em perda parcial de confidencialidade.

Qualquer instância do Kibana configurada com o conector da crowdstrike e a execução de uma versão impactada é vulnerável. Isso inclui configurações nas quais os usuários gerenciam vários espaços para organizar painéis, alertas e conectores.

Elástico Corrigiu a falha nas seguintes versões corrigidas: 8.18.8, 8.19.5, 9.0.8 e 9.1.5. Os usuários que executam versões afetadas devem atualizar para um desses lançamentos sem demora.

Nenhuma solução alternativa ou de mitigação temporária está disponível; portanto, a atualização é a única medida eficaz.

Após a atualização, os administradores devem revisar as configurações do conector para garantir que eles estejam funcionando corretamente e girar quaisquer credenciais que possam ter sido expostas.

Verifique sua versão Kibana e planeje uma atualização para um dos lançamentos fixos. Envolva -se com sua equipe de segurança para verificar a saúde do conector e considerar as chaves da API de crowdstrike rotativas.

Por fim, monitora o canal de anúncios de segurança da Elastic para qualquer orientação ou atualizações adicionais.