Ataque da cadeia de suprimentos "Shai-Halud" Alvos 477 pacotes npm - A

Data: 2025-09-17 06:06:45

Autor: Inteligência Against Invaders

Um grande ataque da cadeia de suprimentos chamado de “Shai-Halud” impactou o ecossistema JavaScript, visando mais de 477 pacotes de NPM, levantando sérias preocupações entre desenvolvedores e organizações que dependem do software do Registro de Gerenciador de Pacotes de Pacote de Node (NPM).

Esse incidente revela a escala e a sofisticação das ameaças modernas ao software de código aberto e destaca a necessidade urgente de melhores medidas de segurança na comunidade de desenvolvimento.

Detalhes de ataque e metas

A campanha Shai-Halud foi detectada pela primeira vez por pesquisadores de segurança que identificaram atividades suspeitas vinculadas a Relacionado com crowdstrike Pacotes NPM.

Os atacantes obtiveram acesso não autorizado a contas de editores confiáveis, permitindo que eles enviem código malicioso para centenas de pacotes legítimos hospedados no NPM.

Alguns dos pacotes comprometidos, incluindo o crowdstrike-api, e vários outros comumente usados ??para integrar a funcionalidade de crowdstrike em soluções de segurança e automação.

Nome do pacote	Versão afetada
@crowdstrike/commitlint	8.1.1
@crowdstrike/commitlint	8.1.2
@Crowdstrike/Falcon-Shoelace	0.4.1
@Crowdstrike/Falcon-Shoelace	0.4.2
@crowdstrike/fundição-js	0,19.1
@crowdstrike/fundição-js	0,19.2
@crowdstrike/glide-core	0,34.2
@crowdstrike/glide-core	0,34.3
@CrowdStrike/LogScale-Dashboard	1.205.1
@CrowdStrike/LogScale-Dashboard	1.205.2
@Crowdstrike/LogScale-File-Editor	1.205.1
@Crowdstrike/LogScale-File-Editor	1.205.2
@crowdstrike/logcale-parser-edit	1.205.1
@crowdstrike/logcale-parser-edit	1.205.2
@Crowdstrike/LogScale-Search	1.205.1
@Crowdstrike/LogScale-Search	1.205.2

Nome do pacote	Versão afetada
@Crowdstrike/Tailwind-Toucan-Base	5.0.1
@Crowdstrike/Tailwind-Toucan-Base	5.0.2

Pesquisadores descobriram que os atacantes aproveitaram as ferramentas de automação para injetar rapidamente pacotes desonestos no registro, explorando a proteção fraca da conta e a supervisão inadequada.

As evidências sugerem que essa foi uma operação coordenada e em larga escala que procurou especificamente pacotes referenciados em ambientes corporativos.

Depois de instalados, os pacotes infectados eram capazes de executar scripts pós-instalação projetados para exfiltrar as variáveis ??e segredos do ambiente.

Ao direcionar pipelines de CI/CD e ambientes de desenvolvimento, os invasores pretendiam roubar tokens de autenticação sensíveis, credenciais de nuvem e arquivos de configuração.

Essa abordagem lhes permitiu obter acesso persistente a redes internas, potencialmente comprometendo aplicativos e dados críticos de negócios.

Especialistas em segurança alertaram isso desde Pacotes NPM são amplamente reutilizados e geralmente têm uma árvore de dependência ampla, os efeitos cascata dos ataques da cadeia de suprimentos como Shai-Halud podem ser vastos.

Se um único pacote estiver comprometido, todo aplicativo e biblioteca, dependendo dele, poderão se tornar vulneráveis.

Os parceiros de registro e segurança da NPM trabalharam rapidamente para identificar e remover os pacotes maliciosos após a descoberta.

Os editores afetados foram notificados e as orientações foram fornecidas para auditoria e atualização de dependências.

Os desenvolvedores que usam integrações de crowdstrike ou pacotes NPM semelhantes devem revisar imediatamente suas listas de dependência, remover quaisquer pacotes sinalizados e redefinir credenciais para ambientes potencialmente expostos.

Este ataque serve como um aviso claro para a cadeia de suprimentos de software mais ampla. Os especialistas recomendam a aplicação da autenticação de vários fatores para contas de editores, monitorando a integridade do pacote e o uso de ferramentas automatizadas de varredura para detectar atividades suspeitas.

Manter a vigilância contra a manipulação da cadeia de suprimentos é agora uma responsabilidade crítica para todas as organizações que dependem de bibliotecas de código aberto.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.