O POC publicado para a falha do sudo permite que os atacantes escalem p

Data: 2025-10-06 05:25:43

Autor: Inteligência Against Invaders

Uma exploração de prova de conceito foi divulgada para CVE-2025-32463, uma vulnerabilidade

crítica de escalada de privilégio local que afeta o binário sudo que permite que os invasores

obtenham acesso de raiz em sistemas Linux.

A falha foi descoberto pelo pesquisador de segurança Rich Mirch e chamou atenção significativa da comunidade de segurança cibernética.

Vulnerabilidade crítica no sudo binário

O CVE-2025-32463 representa uma falha séria de segurança no utilitário sudo amplamente usado, que é fundamental para a administração do sistema Linux.

A vulnerabilidade permite que os usuários locais com privilégios de baixo nível aumentem seu acesso ao nível da raiz, comprometendo efetivamente todo o sistema.

Detalhes da CVE	**Informação**
Cve id	CVE-2025-32463
Componente	Sudo binário
Tipo	Escalada de privilégio local
Versões afetadas	Sudo 1.9.14 a 1.9.17

Esse tipo de ataque de escalada de privilégios apresenta riscos significativos para organizações que executam versões vulneráveis ??do sudo em sua infraestrutura Linux.

A vulnerabilidade afeta especificamente a funcionalidade do chroot no sudo, permitindo que os invasores explorem incorporações incorretas ou usem entradas criadas para ignorar os controles de segurança.

O pesquisador de segurança Mohsen Khashei publicou uma exploração completa de prova de conceito no Github, demonstrando a exploração prática dessa falha.

O repositório de exploração já atraiu considerável atenção com mais de 200 estrelas e quase 30 garfos, indicando interesse generalizado em entender e testar essa vulnerabilidade.

A vulnerabilidade afeta as versões do sudo 1.9.14 a 1.9.17, representando uma parcela significativa das implantações atuais do Linux.

As organizações que administram essas versões específicas enfrentam risco imediato de possíveis

invasores que poderiam alavancar essa falha para ganhar Acesso à raiz não autorizado.

Notavelmente, as versões herdadas anteriores à 1.9.14 permanecem inalteradas, pois o recurso vulnerável de chroot não existia em lançamentos anteriores.

A versão remendada, sudo 1.9.17p1 e libera posterior, aborda completamente essa falha de segurança.

Os administradores do sistema devem priorizar a atualização para a versão mais recente de remendos para eliminar o risco de exploração.

O impacto da vulnerabilidade se estende além dos sistemas individuais, pois o acesso raiz comprometido pode levar ao movimento lateral nos ambientes de rede e ao compromisso completo da infraestrutura.

A ação imediata é necessária para organizações que executam versões vulneráveis ??do sudo. A mitigação primária envolve atualizar o sudo para a versão 1.9.17p1 ou posterior.

Além disso, a implementação de estruturas de segurança, como o Appmor ou o Selinux, pode fornecer camadas adicionais de proteção, limitando o comportamento do sudo e restringindo possíveis tentativas de exploração.

As equipes de segurança também devem implementar o monitoramento para invocações anormais do sudo, o que pode indicar a tentativa de exploração disso vulnerabilidade.

A disponibilidade do código de prova de conceito pública aumenta significativamente a probabilidade de tentativas de exploração, tornando o patches rápido essencial para manter a segurança do sistema.

A vulnerabilidade serve como um lembrete crítico da importância de manter os componentes do sistema atualizados, principalmente para utilitários críticos de segurança como Sudo, que fornecem controles de acesso privilegiados em ambientes Linux.

Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas e definir GBH como uma fonte preferida em** Google**.**