Alerta CISA: Bug Sudo afeta Linux e Unix! Ação urgente necessária até 20

Data: 2025-10-03 07:50:47

Autor: Inteligência Against Invaders

Redazione RHC**:3 Outubro 2025 09:48**

O **Centro de Segurança do Ciberespaço e Infraestrutura (CISA)** recentemente adicionou a vulnerabilidade crítica no utilitário Sudo ao seu **Vulnerabilidades exploradas ativamente (KEV)** lista. Isso efetivamente leva as agências governamentais a *tomar medidas imediatas para resolver o problema.* A lista foi atualizada na segunda-feira com a adição de mais quatro vulnerabilidades.

A vulnerabilidade em questão é CVE-2025-32463 (pontuação de ameaça CVSS 9.3), que afeta todas as versões do Sudo anteriores a 1.9.17p1, em distribuições Linux e sistemas semelhantes ao Unix.

“O Sudo contém uma vulnerabilidade que permite que a funcionalidade de terceiros seja invocada sem verificar o escopo do controle”, afirma a publicação da CISA. ” *Essa vulnerabilidade permite que um invasor local use a opção sudo -R (chroot) para executar comandos arbitrários como root, mesmo que o invasor não esteja presente na lista de usuários sudo.”*

O Centro de Defesa do Ciberespaço e Infraestrutura dos EUA ordenou que as agências governamentais mitigassem as vulnerabilidades no Sudo e em quatro outros produtos de software até 20 de outubro.

Sudo é um utilitário de linha de comando disponível em sistemas Linux e Unix. Ele permite que usuários sem privilégios *executar comandos como administradores ou outros usuários privilegiados.* Isso permite a execução limitada de ações que normalmente exigiriam privilégios administrativos. O arquivo sudoers é uma lista que define as permissões do usuário e os comandos que eles podem executar usando o sudo.

A publicação da CISA **não fornece detalhes sobre como exatamente o** CVE-2025-32463 **vulnerabilidade é explorada** . As informações sobre a vulnerabilidade tornaram-se públicas em julho deste ano, quando o pesquisador da Stratascale **Mirch Rico** publicou sua análise.

É referido que a exploração *foi confirmado em sistemas que executam o Ubuntu 24.04.1 (Sudo 1.9.15p5, Sudo 1.9.16p2) e o Fedora 41 Server (Sudo 1.9.15p5).* A publicação Hacker News também lista as distribuições Linux cujos desenvolvedores e mantenedores emitiram boletins de segurança sobre essa vulnerabilidade: além do Ubuntu, estes incluem *Alpine Linux, Amazon Linux, Debian, Gentoo e Red Hat.*

“Esta não é a primeira vez que bugs são descobertos no sudo” anotações **Alexandre Zonov** , especialista da empresa de processamento de dados SEQ. *“Quando essa infraestrutura crítica,*

especialmente se for extremamente difundida, se torna um elo fraco, as consequências podem ser bastante dramáticas. Portanto, corrigir vulnerabilidades deve ser uma prioridade."

A CISA orienta todas as agências federais dos EUA a tomar medidas para resolver essas vulnerabilidades até 20 de outubro de 2025.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli