



# RegreSSHion CVE-2024-6387: Falha Crítica de Execução Remota de Código no OpenSSH

## Introdução

Em um cenário onde a segurança digital é imperativa, uma nova vulnerabilidade no OpenSSH, identificada como CVE-2024-6387, tem chamado a atenção de administradores de sistemas e profissionais de segurança de todo o mundo. Batizada como "regreSSHion", essa falha grave de segurança permite a execução remota de código (RCE) e pode comprometer seriamente a integridade dos sistemas vulneráveis.

## O que é OpenSSH?

OpenSSH (Open Secure Shell) é um conjunto de utilitários que fornece sessões de rede seguras utilizando o protocolo SSH. Ele é amplamente utilizado em servidores e sistemas operacionais Unix-like para gerenciamento remoto seguro, execução de comandos e transferência de arquivos. Devido à sua popularidade e uso extensivo, qualquer vulnerabilidade no OpenSSH pode ter um impacto significativo e generalizado.

## Mecanismo de Exploração

A vulnerabilidade "regreSSHion" se aproveita de uma regressão introduzida em uma recente atualização do OpenSSH. A falha em questão ocorre no módulo de autenticação, onde a validação inadequada dos dados de entrada permite a execução de ataques format string ou buffer overflow, resultando em corrupção de memória e possibilidade de injeção de código.

## Detalhes da Vulnerabilidade

A CVE-2024-6387 revela uma grave falha no código do OpenSSH que pode ser explorada remotamente, permitindo que um atacante execute código arbitrário no sistema alvo. Isso é conhecido como uma vulnerabilidade de Execução Remota de Código (RCE). Quando explorada com sucesso, essa falha concede ao invasor o controle completo sobre o sistema comprometido, potencialmente levando a roubo de dados, instalação de malware, ou destruição de arquivos.

## Impacto e Adoção

O impacto potencial dessa vulnerabilidade é extremamente alto, dado que o OpenSSH é amplamente utilizado em servidores de produção, roteadores, dispositivos de IoT e muitos outros sistemas críticos. Um ataque bem-sucedido pode levar à perda de dados sensíveis, comprometimento de sistemas e interrupção de serviços.

## Setores atingidos

Servidores de Produção	Infraestrutura de Nuvem	Sistemas Corporativos	Dispositivos de Redes e IoT
Sistemas que utilizam OpenSSH para gerenciamento remoto de servidores são os mais impactados.	Máquinas virtuais e contêineres na nuvem que dependem do OpenSSH para comunicação segura também são vulneráveis.	Qualquer organização que utiliza OpenSSH pode ser um alvo fácil se a vulnerabilidade não for corrigida prontamente.	Roteadores, switches e dispositivos IoT que utilizam OpenSSH estão em risco.

## Mitigação e Patches

A equipe de desenvolvimento do OpenSSH agiu rapidamente para lançar um patch que corrige a vulnerabilidade CVE-2024-6387. Recomenda-se que todos os administradores de sistemas e profissionais de segurança apliquem a atualização mais recente imediatamente para mitigar o risco de exploração.

## Ferramentas para Mitigação by senhasegura®

### Isolamento das sessões SSH por meio do Proxy:

A senhasegura oferece a funcionalidade de proxy, atuando como um intermediário entre o usuário final e o servidor SSH:

- Previne exploração direta da vulnerabilidade, pois os usuários não possuem acesso direto aos servidores;
- Todas as sessões executadas pela senhasegura são monitoradas e podem ser encerradas automaticamente caso comportamentos suspeitos sejam identificados.

### Gravação e auditoria de sessões

Todas as sessões SSH são gravadas e auditadas, incluindo capturas de tela, comandos executados e ações realizadas, que permitem:

- Detecção de atividades suspeitas que possam indicar uma tentativa de exploração;

- Desestimulação das tentativas de exploração, pois o usuário sabe que está sendo monitorado.

### Rotacionamento das credenciais

A senhasegura realiza o rotacionamento de credenciais de maneira periódica e automatizada, garantindo a substituição de senhas antigas e comprometidas. Isso reduz a janela de oportunidade para exploração da vulnerabilidade.

### Acesso Just-In-Time (JIT)

O acesso às credenciais privilegiadas é concedido apenas quando necessário e por um tempo limitado, diminuindo as chances de exploração.

### Políticas de acesso

A definição de políticas de acesso rigorosas, aliada a mecanismos de autenticação multifator (MFA), limita o acesso apenas a usuários devidamente autorizados. Essa combinação garante que somente usuários aprovados, após passarem por uma verificação adicional de identidade, consigam acessar os dispositivos.

## Conclusão

Para ajudar as empresas na validação dos seus ambientes, nosso senhasegura Identity Threat Lab criou uma ferramenta OpenSource que valida se seus servidores estão vulneráveis a essa CVE: <https://github.com/identity-threat-labs/CVE-2024-6387-Vulnerability-Checker>

A vulnerabilidade regreSSHion (CVE-2024-6387) no OpenSSH serve como um lembrete potente da importância de manter sistemas e softwares atualizados, bem como de realizar análises contínuas de segurança. Devido ao potencial devastador dessa falha, é imperativo que os responsáveis pela segurança de sistemas tomem medidas imediatas para aplicar as correções disponíveis e mitigarem qualquer risco potencial. A segurança cibernética é uma responsabilidade coletiva, e a diligência proativa pode prevenir ataques catastróficos.



+55 11 3069-3910

sales@senhasegura.com