BOLETIM DE SEGURANÇA

Vulnerabilidade RCE da regreSSHion no OpenSSH concede acesso root em servidores Linux

heimdall
security research
A DIVISION OF ISH

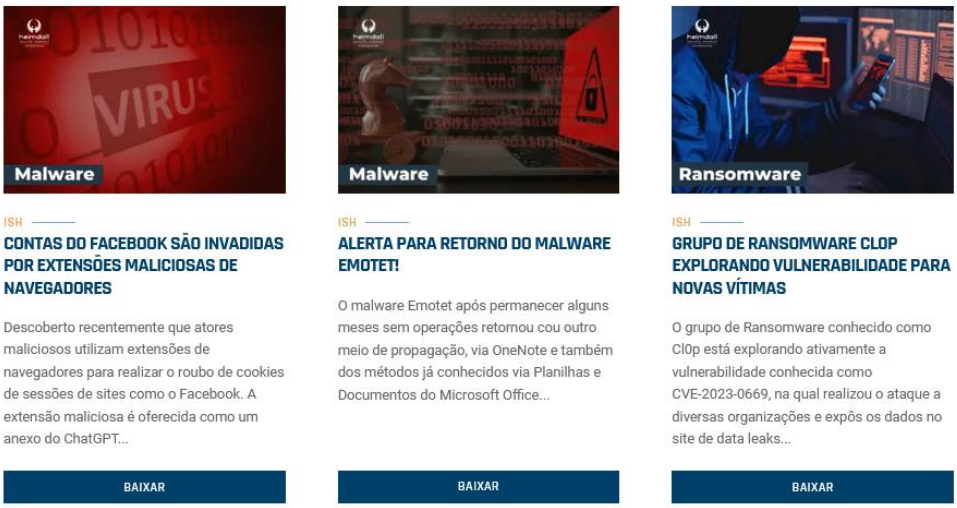
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

1 SUMÁRIO EXECUTIVO

Pesquisadores da Qualys descobriram uma nova vulnerabilidade CVE-2024-6387 não autenticada de execução remota de código (RCE) no OpenSSH, denominada regreSSHion, permitindo a obtenção de privilégios de root em sistemas Linux que utilizam glibc.

2 DETALHES SOBRE A VULNERABILIDADE

A Vulnerabilidade CVE-2024-6387 categorizada como alta que afeta o servidor OpenSSH (sshd). Ela é caracterizada por uma condição de corrida no manipulador de sinais, permitindo a execução remota de código (RCE) sem autenticação como root em sistemas Linux que utilizam glibc. Isso representa um risco de segurança considerável, pois a condição de corrida afeta o sshd em sua configuração padrão.

Pesquisas realizadas com o uso de Censys e Shodan revelaram a existência de mais de 14 milhões de instâncias de servidor OpenSSH potencialmente vulneráveis expostas à Internet. Dados anonimizados do Qualys CSAM 3.0, juntamente com informações do External Attack Surface Management, indicam que cerca de 700.000 dessas instâncias externas voltadas para a Internet são vulneráveis. Isso equivale a 31% de todas as instâncias de OpenSSH voltadas para a Internet em nossa base global de clientes. Notavelmente, mais de 0,14% dessas instâncias vulneráveis estão executando uma versão do OpenSSH que já atingiu o fim de sua vida útil ou suporte.

Essa vulnerabilidade foi identificada como uma regressão da vulnerabilidade CVE-2006-5051, que foi corrigida em 2006. Uma regressão, neste contexto, significa que um defeito que havia sido corrigido reapareceu em uma versão subsequente do software, geralmente devido a alterações ou atualizações que reintroduziram o problema inadvertidamente. Este incidente ressalta a importância crucial de realizar testes de regressão completos para evitar a reintrodução de vulnerabilidades conhecidas no ambiente. Esta regressão específica foi introduzida em outubro de 2020.

OpenSSH (**Open Secure Shell**) é uma suíte de utilitários de rede que oferece uma camada segura de comunicação em redes inseguras, baseada no protocolo Secure Shell (SSH). Ele é conhecido por sua criptografia robusta, que garante a privacidade e a segurança na transferência de arquivos. Isso o torna uma ferramenta indispensável para o gerenciamento remoto de servidores e a comunicação segura de dados. O OpenSSH é reconhecido por seus recursos de segurança e autenticação abrangentes, suportando diversas tecnologias de criptografia. Ele é padrão em vários sistemas semelhantes ao Unix, incluindo macOS e Linux.

A implementação do OpenSSH é uma ferramenta essencial para a comunicação segura. Seu valor para as empresas reside em sua escalabilidade e na capacidade de impor controles de acesso robustos, protegendo processos automatizados em diversos ambientes. Isso abrange desde backups automatizados e processamento em lote até práticas complexas de DevOps, que envolvem o manuseio seguro de dados confidenciais em vários sistemas e locais.

O desenvolvimento contínuo do OpenSSH e sua ampla adoção sublinham sua importância na manutenção da confidencialidade e integridade das comunicações de rede em todo o mundo. O OpenSSH é um marco na segurança de software, exemplificando uma abordagem robusta de defesa em profundidade. Apesar de uma recente vulnerabilidade, seu histórico geral permanece excepcionalmente forte, servindo como modelo e inspiração no campo da segurança cibernética.

As versões do OpenSSH que antecedem a 4.4p1 são suscetíveis a uma condição de corrida do manipulador de sinais, a menos que tenham sido corrigidas para os CVE-2006-5051 e CVE-2008-4109. As versões que vão da 4.4p1 até a 8.5p1, excluindo esta última, estão imunes a essa vulnerabilidade graças a um patch transformador para o CVE-2006-5051, que tornou segura uma função que antes era insegura. No entanto, a vulnerabilidade reaparece nas versões que vão da 8.5p1 até a 9.8p1, excluindo esta última, devido à remoção acidental de um componente crucial em uma função. Os sistemas OpenBSD não são impactados por esse bug, pois o OpenBSD implementou um mecanismo seguro em 2001 que impede essa vulnerabilidade.

Caso essa vulnerabilidade for explorada, pode resultar em um comprometimento total do sistema. Um invasor poderia executar código arbitrário com os privilégios mais altos, levando a uma tomada de controle total do sistema, instalação de malware, manipulação de dados e criação de backdoors para acesso contínuo. Isso poderia facilitar a propagação pela rede, permitindo que invasores usem um sistema comprometido como um trampolim para explorar outros sistemas vulneráveis dentro da organização.

Além disso, o acesso root permitiria que os invasores contornassem mecanismos de segurança críticos, como firewalls, sistemas de detecção de intrusão e mecanismos de registro, tornando suas atividades ainda mais obscuras. Isso também poderia levar a violações significativas de dados e vazamentos, dando aos invasores acesso a todos os dados armazenados no sistema, incluindo informações confidenciais ou proprietárias que poderiam ser roubadas ou divulgadas publicamente.

Essa vulnerabilidade é desafiadora de explorar devido à sua natureza de condição de corrida remota, exigindo várias tentativas para um ataque bem-sucedido. Isso pode levar à corrupção de memória e à necessidade de superar o Address Space Layout Randomization (ASLR). Avanços no aprendizado profundo podem aumentar significativamente a taxa de exploração, potencialmente fornecendo aos invasores uma vantagem substancial ao explorar tais falhas de segurança.

3 RECOMENDAÇÕES

A Qualys recomenda que seja realiza as etapas abaixo para que seja possível a mitigação dessa vulnerabilidade.

Gerenciamento de patches

- Aplique rapidamente os patches disponíveis para o OpenSSH e priorize os processos de atualização em andamento.

Controle de acesso aprimorado

- Limite o acesso SSH por meio de controles baseados em rede para minimizar os riscos de ataque.

Segmentação de rede e detecção de intrusão

- Divida redes para restringir acesso não autorizado e movimentos laterais em ambientes críticos e implante sistemas para monitorar e alertar sobre atividades incomuns indicativas de tentativas de exploração.

Avaliação e correção personalizadas

- Execute rapidamente o script de mitigação nos ativos necessários.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Qualys**
- **Bleepingcomputer**
- **NVD**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH