BOLETIM DE SEGURANÇA

Descoberta nova falha de segurança no OpenSSH ameaça execução de código remoto

heimdall
security research
A DIVISION OF ISH

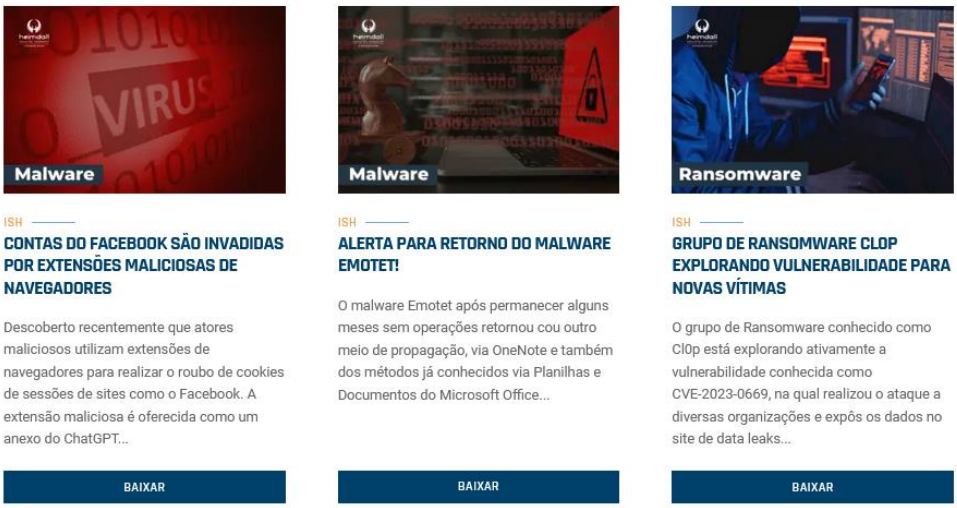
TLP: CLEAR

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

Foi descoberta uma nova vulnerabilidade no OpenSSH, rastreada como CVE-2024-6409, é distinta da CVE-2024-6387 (também conhecida como *RegreSSHion*) e se relaciona a um caso de execução de código no processo filho privsep devido a uma condição de corrida no tratamento de sinal.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A vulnerabilidade, identificada como CVE-2024-6409 possui uma pontuação CVSS de 7.0, é diferente do CVE-2024-6387, também conhecido como RegreSSHion. Ela está relacionada a um caso de execução de código no processo filho privsep devido a uma condição de corrida no tratamento de sinal. A vulnerabilidade afeta apenas as versões 8.7p1 e 8.8p1 do Red Hat Enterprise Linux 9.

Alexander Peslyak, um pesquisador de segurança, foi reconhecido pela descoberta e relato do bug. Este bug foi identificado durante uma revisão do CVE-2024-6387, que foi divulgado pela Qualys recentemente. Peslyak destacou que a principal diferença em relação ao CVE-2024-6387 é que a condição de corrida e o potencial RCE são acionados no processo filho privsep. Este processo é executado com privilégios reduzidos em comparação ao processo do servidor pai.

Embora o impacto imediato seja menor, Peslyak observou que podem existir diferenças na capacidade de exploração dessas vulnerabilidades em um cenário específico. Isso pode tornar qualquer uma delas mais atraente para um invasor. Se apenas uma delas for corrigida ou mitigada, a outra se torna mais relevante. É importante notar que a vulnerabilidade de condição de corrida do manipulador de sinal é a mesma do CVE-2024-6387. Se um cliente não for autenticado dentro de LoginGraceTime segundos (120 por padrão), o manipulador SIGALRM do processo daemon OpenSSH será chamado de forma assíncrona. Isso invoca várias funções que não são seguras para sinais assíncronos.

Este problema torna o sistema vulnerável a uma condição de corrida do manipulador de sinal na função cleanup_exit(). Isso introduz a mesma vulnerabilidade que CVE-2024-6387 no filho sem privilégios do servidor SSHD, conforme descrito na descrição da vulnerabilidade. No caso de um ataque bem-sucedido, o cenário mais grave permitiria ao invasor executar código remotamente (RCE) dentro de um usuário sem privilégios que esteja operando o servidor sshd. Desde então, foi identificado um exploit ativo para CVE-2024-6387. Um agente de ameaça não identificado tem como alvo principal servidores situados na China.

3 RECOMENDAÇÕES

Mantenha seus dispositivos e software atualizados

- Instale regularmente atualizações de segurança em seus sistemas operacionais, aplicativos e dispositivos.

Utilize ativos de segurança

- Use firewalls e antimalware sempre atualizados para proteção contra ameaças, inclusive de endpoints.

Implemente uma política de mínimo privilégio

- Permita aos usuários exercer ações na rede restritas ao desempenho de suas funções organizacionais.

Bloqueie o tráfego da porta 445/SMB

- Até que as atualizações sejam instaladas, bloqueie o tráfego da porta 445/SMB para fora da rede.

Recurso de grupo do Active Directory

- Utilize este recurso para as contas dos administradores de domínio.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Thehackernews**
- **NVD**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH