BOLETIM DE SEGURANÇA

FreeBSD lança atualização emergencial para falha grave no OpenSSH

heimdall
security research
A DIVISION OF ISH

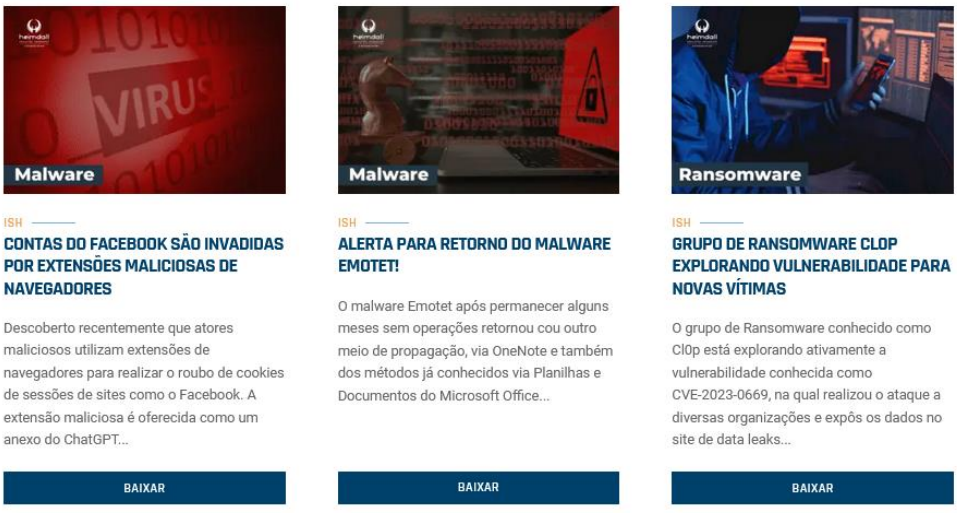
TLP: CLEAR

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

Os responsáveis pelo Projeto FreeBSD divulgaram atualizações de segurança para corrigir uma falha grave no OpenSSH. Essa vulnerabilidade, identificada como CVE-2024-7589, possui uma pontuação CVSS de 8.1, indicando alta gravidade. Invasores poderiam explorar essa falha para executar código arbitrário remotamente com privilégios elevados.

2 DETALHES DA VULNERABILIDADE

Esta vulnerabilidade afeta o OpenSSH no FreeBSD. O problema está em um manipulador de sinal no **sshd(8)** que pode chamar uma função de log não segura de forma assíncrona quando um cliente falha na autenticação dentro do tempo configurado em *LoginGraceTime*. O manipulador de sinal executa com privilégios de root, resultando em uma possível condição de corrida que um determinado invasor pode explorar para permitir uma execução remota de código não autenticada como root.

3 RECOMENDAÇÕES

Conforme nota dos responsáveis pelo projeto, podem ser adotadas as seguintes recomendações abaixo.

Atualize seu sistema vulnerável para um FreeBSD estável ou release/branch de segurança (releng) com suporte datado após a data de correção e reinicie o sshd.

Atualização do sistema vulnerável por meio de um patch binário:

Sistemas executando uma versão RELEASE do FreeBSD nas plataformas amd64 ou arm64, ou a plataforma i386 no FreeBSD 13, podem ser atualizados por meio do utilitário freebsd-update(8):

- *# freebsd-update fetch*
- *# freebsd-update install*

Atualização do sistema vulnerável por meio de um patch de código-fonte:

Os seguintes patches foram verificados para se aplicar aos branches de release aplicáveis do FreeBSD.

a) Baixe o patch relevante do local abaixo e verifique a assinatura PGP desanexada usando seu utilitário PGP.

- *# fetch https://security.FreeBSD.org/patches/SA-24:08/openssh.patch*
- *# fetch https://security.FreeBSD.org/patches/SA-24:08/openssh.patch.asc*
- *# gpg --verify openssh.patch.asc*

b) Aplique o patch. Execute os seguintes comandos como root:

- *# cd /usr/src*
- *# patch < /path/to/patch*

c) Recompile o sistema operacional usando buildworld e installworld conforme em FreeBSD.

Reinicie os daemons aplicáveis ou reinicialize o sistema.

Em casos onde sshd(8) não pode ser atualizado, o problema de condição de corrida pode ser resolvido definindo *LoginGraceTime* como **0** em */etc/ssh/sshd_config* e reiniciando *sshd(8)*. **Embora essa alteração torne o daemon vulnerável a uma negação de serviço, ela o protege contra execução remota de código.**

4 REFERÊNCIAS

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

5 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH