BOLETIM DE SEGURANÇA

Ator malicioso vendendo exploit de Command Injection no OpenSSH versão 9.6

heimdall
security research
A DIVISION OF ISH

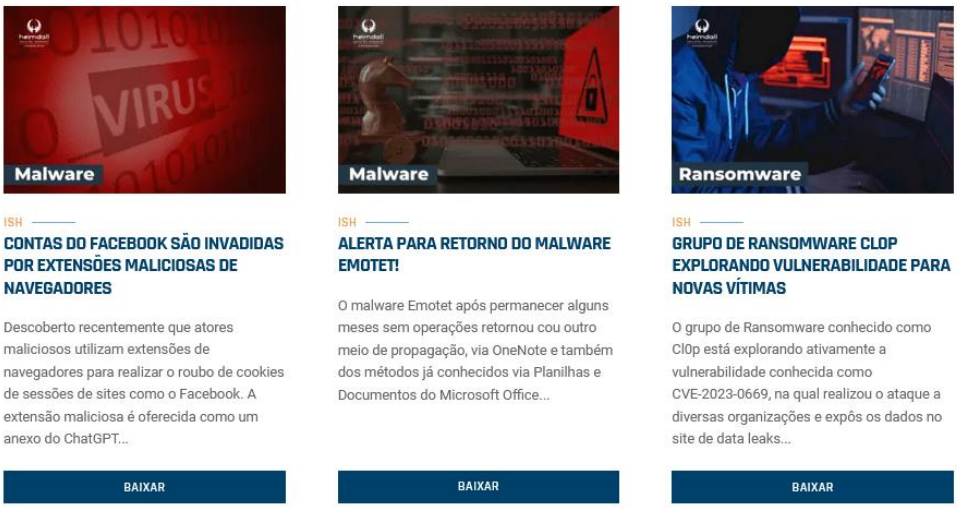
TLP: CLEAR

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

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Foi observado recentemente em fórum “hacker” um ator malicioso realizando a venda de uma possível exploração de Command Injection no OpenSSH na versão 9.6, conforme o anuncio do mesmo, o código pode ser utilizado remotamente (RCE), e afirma que esse exploit foi testado e comprovado como funcional.

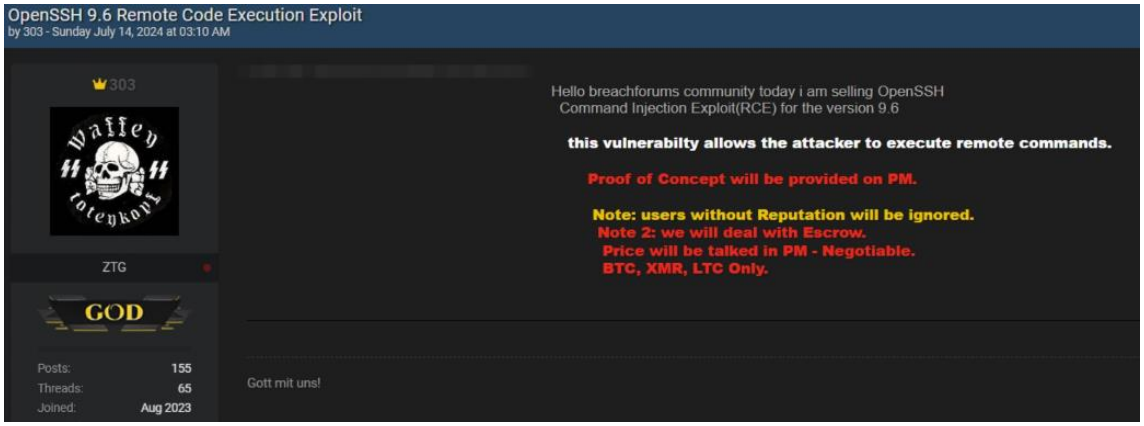


Figura 1 – Publicação e venda do ator malicioso.

Devido à alta usabilidade e explorações anteriores do OpenSSH por atores maliciosos, é requirida uma notável atenção.

2 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

Atualização e patching

- Atualização do OpenSSH: Atualize para a versão mais recente que corrige a falha.
- Verificação de patches: Regularmente verifique por patches de segurança e aplique-os assim que forem disponibilizados.

Configuração de segurança

- Restrição de acesso: Limite o acesso ao servidor SSH somente a endereços IP confiáveis. Utilize um firewall para restringir o acesso.
- Desabilitação de Root login: Desabilite o login direto do usuário root através do SSH (PermitRootLogin no no arquivo de configuração do SSH).
- Utilização de portas não-padrão: Configure o SSH para operar em uma porta diferente da padrão (22) para reduzir a exposição a ataques automatizados.

Monitoramento e detecção

- Monitoramento de logs: Implemente o monitoramento contínuo dos logs do SSH para detectar tentativas de acesso suspeitas.
- Sistema de Detecção de Intrusões (IDS): Utilize sistemas de detecção e prevenção de intrusões para identificar atividades maliciosas.

Hardening do sistema

- Segregação de redes: Segmente a rede para isolar o servidor SSH de outras partes da infraestrutura.
- Redução de superfície de ataque: Desabilite serviços e portas desnecessárias no servidor para minimizar as oportunidades de exploração.

Ações proativas

- Análise de vulnerabilidades: Realize testes regulares de penetração e varreduras de vulnerabilidade para identificar e corrigir falhas de segurança.
- Treinamento de equipe: Garanta que a equipe de TI esteja treinada e ciente das melhores práticas de segurança e da importância de aplicar patches rapidamente.

Resposta a incidentes

- Plano de resposta a incidentes: Tenha um plano de resposta a incidentes bem definido para lidar rapidamente com uma potencial exploração.

- Backup e recuperação: Mantenha backups regulares e testados dos sistemas críticos para assegurar uma recuperação rápida em caso de comprometimento.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **OpenSSH**

4 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH