



BOLETIM DE SEGURANÇA

Vulnerabilidade de ataque de recuperação de
chave encontrada em cliente Putty



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](#)



ISH

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

1	Sumário Executivo	4
2	Informação sobre a vulnerabilidade	5
3	Recomendações.....	6
4	Referências	7

1 SUMÁRIO EXECUTIVO

Pesquisadores de segurança, informaram sobre uma vulnerabilidade [CVE-2024-31497](#) encontrada no cliente Putty comprometendo a chave privada. Em que um atacante que detém um conjunto de mensagens assinadas e a respectiva chave pública pode ter os meios para deduzir a chave privada correspondente. Com essa chave, seria possível forjar assinaturas como se fossem do legítimo proprietário, possibilitando, por exemplo, o acesso a servidores protegidos por essa chave. A aquisição dessas assinaturas pode ser feita através de um comprometimento temporário de qualquer servidor que utilize a chave para autenticação ou por meio de um acesso breve ao Pageant que a armazena. Vale ressaltar que essas assinaturas não ficam vulneráveis a interceptações passivas em conexões SSH.

2 INFORMAÇÃO SOBRE A VULNERABILIDADE

A vulnerabilidade CVE-2024-31497 no PuTTY permite que um invasor descubra a chave secreta de chaves NIST P-521 após observar aproximadamente 60 assinaturas ECDSA. Embora as assinaturas sejam protegidas pelo canal seguro do SSH, um servidor comprometido poderia obter essas assinaturas. Além disso, se a chave foi usada fora do SSH, como em commits do git, as assinaturas podem ser acessadas publicamente, aumentando o risco. Portanto, todas as chaves NIST P-521 utilizadas com PuTTY são consideradas inseguras, e o risco persiste mesmo após correções no código-fonte, caso assinaturas anteriores estejam disponíveis para o atacante.

A falha de segurança foi corrigida nas versões atualizadas do **PuTTY**, **FileZilla**, **WinSCP** e **TortoiseGit**. Para o **TortoiseSVN**, é aconselhável utilizar o Plink do PuTTY 0.81 para conexões SVN via SSH até que um patch seja lançado. A solução envolveu a adoção da técnica [RFC 6979](#) para geração de nonces em chaves DSA e ECDSA, substituindo o método anterior que era vulnerável a nonces previsíveis com o uso da curva P-521. Chaves ECDSA NIST-P521 que foram usadas com os softwares afetados devem ser revogadas e removidas dos arquivos de chaves autorizadas em servidores SSH.

3 RECOMENDAÇÕES

Para mitigar a vulnerabilidade, o método de geração de k do PuTTY foi substituído pela técnica RFC 6979 para chaves DSA e ECDSA. As chaves EdDSA, incluindo Ed25519, já operavam com um sistema distinto e não sofreram alterações. Contudo, é importante ressaltar que as chaves privadas P521 podem ter sido expostas devido ao uso do gerador k anterior nas assinaturas.

4 REFERÊNCIAS

- Heimdall by ISH Tecnologia
- [OpenWall](#)
- [Seclist](#)
- [NVD](#)
- [Thehackernews](#)



heimdall
security research

A DIVISION OF ISH