TLP: CLEAR

BOLETIM DE SEGURANÇA

Falha de segurança no TeamViewer para Windows permite elevação de privilégios

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

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 INTRODUÇÃO EXECUTIVA

Uma vulnerabilidade, identificada como **CVE-2025-0065** de gravidade alta, foi recentemente descoberta no **TeamViewer para Windows**. Essa falha de segurança permite que atacantes locais explorem uma brecha no sistema para elevar seus privilégios, obtendo potencialmente acesso administrativo ou de alto nível no dispositivo afetado.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A vulnerabilidade, registrada como CVE-2025-0065, está presente no componente *TeamViewer_service.exe*, onde ocorre uma neutralização inadequada de delimitadores de argumentos. Isso permite que um atacante com acesso local não privilegiado injete argumentos maliciosos, resultando na elevação de privilégios no sistema Windows afetado. A exploração bem-sucedida dessa falha pode conceder ao atacante controle total sobre o sistema comprometido.

2.1 SISTEMAS E PRODUTOS AFETADOS

A vulnerabilidade afeta as seguintes ferramentas e versões:

- **TeamViewer Full Client para Windows**: Versões anteriores à *15.62*
- **TeamViewer Host para Windows**: Versões anteriores à *15.62*

2.2 IMPACTO DA VULNERABILIDADE

Os principais impactos da vulnerabilidade no TeamViewer incluem:

- Elevação de privilégios
- Execução de comandos arbitrários
- Comprometimento de dados sensíveis

Devido à grande utilização do software, essa falha exige uma atenção especial em termos de proteção.

3 RECOMENDAÇÕES

Para reduzir os riscos decorrentes dessa vulnerabilidade, é aconselhável adotar as seguintes medidas:

Atualizar o software

- Aplicar a versão *15.62* ou superior, onde a vulnerabilidade foi corrigida.

Revisar privilégios de usuário

- Limitar o uso de contas com privilégios administrativos. Usuários devem operar com contas de usuário padrão sempre que possível, elevando privilégios apenas quando necessário.

Monitorar acessos remotos

- Implementar logs de auditoria e monitoramento contínuo para detectar tentativas de exploração.

Aplicar políticas de segurança adicionais

- Restringir a execução do TeamViewer a contas devidamente autorizadas e exigir autenticação multifator (MFA) sempre que possível.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **TeamViewer**
- **NVD**
- **GBHackers**

5 AUTORES

- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH