Vulnerabilidade do cliente Netskope Windows permite a escalada de privil

Data: 2025-08-31 17:09:00

Autor: Inteligência Against Invaders

Uma séria vulnerabilidade de segurança no cliente do Windows do Netskope foi descoberta que

poderia permitir que os invasores escalem privilégios de um usuário de baixo privilégio para o

acesso completo no nível do sistema.

A falha, rastreada como CVE-2025-0309, afeta todas as versões do cliente NetSkope Windows antes da versão R129 e levou a empresa a lançar atualizações de segurança urgentes.

Explorando a Trust Rogue Server

A vulnerabilidade gira em torno do processo de inscrição do cliente Netskope, que os pesquisadores de segurança Richard Warren e David Cash de Amber Wolf encontraram pode ser manipulado através de uma sofisticada cadeia de ataques.

A exploração aproveita a comunicação entre o processo de interface do usuário do cliente baixo (Stagentui) e o serviço privilegiado (StagentsVC) que é executado com privilégios do sistema.

O processo de ataque envolve várias etapas importantes:

- Os atacantes criam um token da Web JSON especialmente formatado (JWT) contendo um URL do servidor Rogue.
- O token malicioso é enviado através do canal de comunicação entre processos (IPC) do cliente usando o ID de comando 148.
- O serviço privilegiado começa a fazer solicitações ao servidor falso do invasor, em vez da infraestrutura legítima do Netskope.
- O servidor Rogue responde com configurações maliciosas e instala uma autoridade de certificação fraudulenta.
- Um backdoord Atualização de software é servido que parece legítimo devido à cadeia fiduciária comprometida.

O servidor Rogue pode então responder com configurações maliciosas, incluindo a instalação de uma autoridade de certificação fraudulenta no armazenamento de raiz confiável do sistema e servir uma atualização de software em backdoor.

Como o invasor controla a autoridade de certificação, eles podem assinar instaladores de software maliciosos que parecem legítimos para as verificações de segurança do cliente.

As proteções internas do cliente, incluindo verificação de assinatura e verificação de digestão, podem ser ignoradas, pois o invasor tem controle total sobre os certificados de assinatura e as

respostas do servidor.

Técnicas de evasão derrota a segurança

Os pesquisadores descobriram várias maneiras de contornar as proteções de segurança do Netskope. O cliente tenta autenticar os chamadores do IPC, verificando se as solicitações vêm de processos legítimos do NetSkope localizados em diretórios protegidos.

No entanto, essa proteção pode ser ignorada pela injeção de código em processos aprovados como nsdiag.exe e usá -los como proxy para comunicações maliciosas do IPC.

Até o recurso “Tiperiper Proof” da Netskope, projetado para evitar o acesso não autorizado a processos protegidos por meio de proteções de motorista no nível do kernel, podem ser derrotadas.

Os pesquisadores desenvolvido Uma técnica que cria um novo processo Netskope em um estado suspenso, substitui as funções críticas do sistema com código malicioso e retoma a execução para carregar sua carga útil de ataque.

Além disso, versões mais recentes do cliente que criptografaram as comunicações IPC não são imunes a esse ataque.

A criptografia usa valores obtidos facilmente do registro do Windows como chave de criptografia e vetor de inicialização, permitindo que os invasores descriptografem e criem mensagens criptografadas.

Netskope emite patches e orientações

O Netskope tomou medidas rápidas para lidar com essa vulnerabilidade crítica. Em 13 de agosto de 2025, a empresa lançou a versão R129 de seus Cliente Windowsque implementa uma lista de permissões codificados de domínios legítimos do NetSkope para impedir a inscrição com servidores desonestos.

A empresa também publicou o Security Advisory NSKPSA-2025-002, fornecendo informações detalhadas sobre a vulnerabilidade.

As organizações que usam o Netskope são fortemente aconselhadas a atualizar para a versão R129 imediatamente.

A empresa também forneceu métodos de detecção para equipes de segurança, incluindo o monitoramento de certificados suspeitos na loja de raizs confiável, observando instalações incomuns do MSI do serviço Netskope e revisando arquivos de log para URLs de addon inesperados ou IDs de inquilino que podem indicar tentativas de compromisso.

Essa vulnerabilidade destaca os complexos desafios de segurança enfrentados pelo software de segurança corporativa, onde a necessidade de acesso privilegiado ao sistema para fornecer proteção também pode criar metas atraentes para os atacantes.

A natureza sofisticada desse ataque, exigindo um profundo conhecimento técnico dos protocolos de arquitetura e comunicação do cliente, sugere que seria principalmente interessante para atores de

ameaças persistentes avançados ou pesquisadores de segurança, em vez de criminosos cibernéticos comuns.

Encontre esta notícia interessante! Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas!**