Vulnerabilidade no protocolo RPC do Windows: ataques de falsificação e f

Data: 2025-09-21 19:55:40

Autor: Inteligência Against Invaders

Redazione RHC**:21 Setembro 2025 20:57**

Especialistas em SafeBreach revelaram detalhes de uma vulnerabilidade no **Chamada de Procedimento Remoto (RPC) do Windows** , corrigido pela Microsoft na atualização de julho de 2025. A falha, CVE-2025-49760, permitiu que um invasor realizasse ataques de falsificação e se passasse por um servidor legítimo usando o mecanismo de armazenamento do Windows. Ron Ben Yizak Discutido a descoberta na conferência DEF CON 33.

O protocolo RPC depende de identificadores de interface exclusivos (UUIDs) e do serviço Endpoint Mapper (EPM), que mapeia as solicitações do cliente para os endpoints dinâmicos dos servidores registrados. A vulnerabilidade Aberto o caminho para um chamado **Ataque de envenenamento por EPM** , no qual um usuário sem privilégios pode registrar uma interface no serviço incorporado e forçar o processo protegido a se autenticar em um servidor arbitrário. Semelhante à falsificação de DNS, o ataque altera o mapeamento de UUIDs para endpoints, redirecionando o cliente para uma fonte falsa.

O problema é agravado pelo fato de que o EPM não verifica a autenticidade do registrador de interface. Isso permitiu que uma interface pertencente a um serviço atrasado ou iniciado manualmente fosse capturada antes que o processo real a registrasse. Isso permitiu que um invasor sequestrasse a conexão sem direitos de administrador.

O SafeBreach criou uma ferramenta chamada RPC-Racer que poderia *detectar serviços RPC inseguros, como o Serviço de Armazenamento (StorSvc.dll), e redirecionar solicitações de um processo PPL seguro, como a Otimização de Entrega (DoSvc.dll), para um servidor SMB controlado por invasores.* Isso faria com que o processo fosse autenticado com a conta do computador passando um hash NTLM, que poderia ser usado em um ataque ESC8 para elevar privilégios por meio dos Serviços de Certificados do Active Directory (ADCS). Usando ferramentas como Certipy, eles foram capazes de obter o *TGT Kerberos e acessar todos os segredos do controlador de domínio* .

Todo o ciclo de ataque incluiu **Criando uma tarefa para ser executada no login do usuário, registrando a interface do serviço de armazenamento** , **disparar uma chamada de Otimização de Entrega para um servidor fictício, enviar um link SMB para um recurso mal-intencionado e extrair o hash NTLM. Os dados NTLM foram usados para obter um certificado e atribuir direitos no nível do domínio.**

Além do escalonamento direto, o envenenamento de EPM pode ser usado para ataques Man-in-the-Middle (MitM), redirecionando solicitações para o serviço original ou para ataques de negação de

serviço, registrando várias interfaces e bloqueando solicitações. O SafeBreach aponta que outros clientes no sistema podem estar vulneráveis a esse sequestro.

Para detectar esses ataques, é recomendável monitorar chamadas RpcEpRegister e usar o ETW (Rastreamento de Eventos para Windows) para capturar eventos gerados por aplicativos e drivers. De acordo com os pesquisadores, semelhante à forma como a fixação SSL verifica uma chave específica, o EPM deve verificar a identidade do servidor RPC, caso contrário, os clientes confiarão em fontes não verificadas.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli