Investigadores en ciberseguridad han revelado nuevos hallazgos sobre una vulnerabilidad ya corregida en el protocolo de comunicación Windows Remote Procedure Call (RPC) de Microsoft, la cual podría ser aprovechada por un atacante para realizar ataques de suplantación y hacerse pasar por un servidor legítimo.

El fallo, identificado como CVE-2025-49760 (con una puntuación CVSS de 3.5), fue descrito por la compañía tecnológica como un error de suplantación en Windows Storage. Se solucionó en julio de 2025 dentro de las actualizaciones mensuales del Patch Tuesday. Los detalles fueron expuestos por el investigador de SafeBreach, Ron Ben Yizhak, durante la conferencia de seguridad DEF CON 33 esta semana.

"El control externo del nombre o ruta de archivo en Windows Storage permite a un atacante autorizado realizar suplantación a través de la red", indicó la empresa en un aviso publicado el mes pasado.

El protocolo Windows RPC utiliza identificadores únicos universales (UUIDs) y un mapeador de puntos finales (Endpoint Mapper o EPM) para habilitar el uso de endpoints dinámicos en la comunicación cliente-servidor, conectando un cliente RPC con un endpoint registrado por un servidor.

La vulnerabilidad, en esencia, permite manipular un componente clave del protocolo RPC y llevar a cabo un ataque de envenenamiento de EPM, lo que posibilita que usuarios sin privilegios se hagan pasar por un servicio legítimo del sistema con el fin de forzar que un proceso protegido se autentique contra un servidor arbitrario controlado por el atacante.

Dado que el funcionamiento del EPM es similar al del Sistema de Nombres de Dominio (DNS) —mapeando un UUID de interfaz a un endpoint, del mismo modo que el DNS resuelve un dominio a una dirección IP—, el ataque se asemeja a un envenenamiento DNS, donde un actor malicioso altera los datos de DNS para redirigir a las víctimas a sitios web peligrosos.

Secuencia básica del ataque:

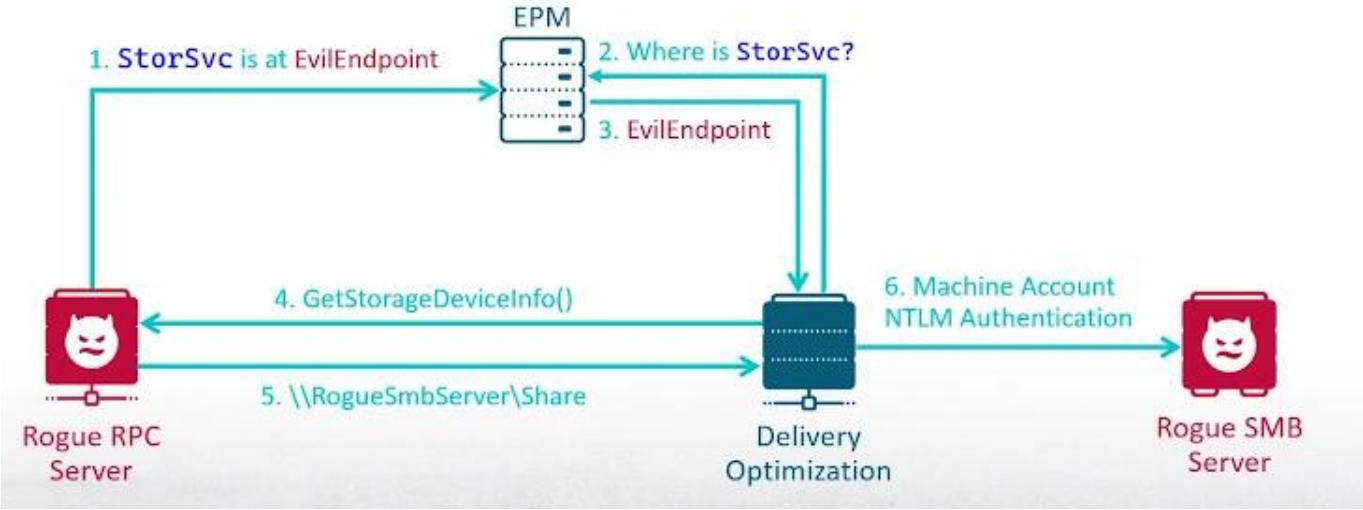
- Envenenar el EPM
- Hacerse pasar por un servidor RPC legítimo
- Manipular clientes RPC
- Escalar privilegios locales o de dominio mediante un ataque ESC8

"Me sorprendió descubrir que no había nada que impidiera registrar interfaces conocidas, integradas, que pertenecen a servicios esenciales", explicó Ben Yizhak en un informe compartido con The Hacker News. *"Esperaba, por ejemplo, que si Windows Defender tenía un identificador único, ningún otro proceso pudiera registrarlo. Pero no fue así"*.

"Cuando intenté registrar la interfaz de un servicio que estaba desactivado, su cliente se conectó a mí en su lugar. Este hallazgo fue increíble: el EPM no realizó ninguna verificación de seguridad. Conectó clientes a un proceso desconocido que ni siquiera se ejecutaba con privilegios de administrador".

El núcleo del ataque consiste en identificar interfaces que no estén asignadas a un endpoint, así como aquellas que puedan registrarse justo después de iniciar el sistema, aprovechando que muchos servicios están configurados con "inicio retrasado" para mejorar el rendimiento y acelerar el arranque.

En otras palabras, cualquier servicio con inicio manual representa un riesgo, ya que su interfaz RPC no se registrará al arrancar, lo que deja abierta la posibilidad de que un atacante se adelante y la registre antes que el servicio original.



SafeBreach también presentó una herramienta llamada RPC-Racer, diseñada para detectar servicios RPC inseguros (por ejemplo, Storage Service o StorSvc.dll) y manipular procesos Protected Process Light (PPL), como Delivery Optimization o DoSvc.dll, para que se autentiquen con una cuenta de máquina contra cualquier servidor definido por el atacante.

La tecnología PPL garantiza que el sistema operativo solo cargue servicios y procesos de confianza, protegiéndolos contra su terminación o infección por código malicioso. Microsoft la introdujo con Windows 8.1.

Resumen de la secuencia de ataque:

1. Crear una tarea programada para ejecutarse cuando el usuario actual inicie sesión
2. Registrar la interfaz del servicio Storage
3. Forzar que Delivery Optimization envíe una solicitud RPC a Storage, provocando que se conecte al endpoint dinámico del atacante
4. Invocar el método `GetStorageDeviceInfo()`, lo que lleva a que Delivery Optimization reciba un recurso SMB malicioso controlado por el atacante
5. Delivery Optimization se autentica en el servidor SMB con las credenciales de la cuenta de máquina, filtrando el hash NTLM

6. Realizar un ataque ESC8 para reenviar los hashes NTLM a los servicios web de inscripción de certificados (AD CS) y escalar privilegios

Para completar este ataque, puede utilizarse una herramienta ofensiva de código abierto como Certipy, la cual solicita un Ticket-Granting Ticket (TGT) de Kerberos usando un certificado generado a partir de la información NTLM obtenida, y posteriormente permite extraer todos los secretos del controlador de dominio.

SafeBreach advirtió que la técnica de envenenamiento EPM podría ampliarse para realizar ataques de *adversario-en-el-medio* (AitM) y de denegación de servicio (DoS), reenviando solicitudes al servicio original o registrando múltiples interfaces para bloquear las peticiones, respectivamente. La empresa también señaló que es probable que existan otros clientes e interfaces vulnerables a este tipo de ataque.

Para mejorar la detección, las soluciones de seguridad pueden monitorear llamadas a `RpcEpRegister` y emplear *Event Tracing for Windows* (ETW), una función que registra eventos generados por aplicaciones en modo usuario y controladores en modo kernel.

"Así como el SSL pinning verifica que un certificado no solo sea válido sino que use una clave pública específica, también debería comprobarse la identidad de un servidor RPC", afirmó Ben Yizhak.

"El diseño actual del endpoint mapper (EPM) no realiza esa verificación. Sin ella, los clientes aceptan datos de fuentes desconocidas. Confiar ciegamente en esa información permite a un atacante controlar las acciones del cliente y manipularlo a su antojo".