Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

TETÃ REKUÁI GOBIERNO NACIONAL

BOLETÍN DE ALERTA

Boletín Nro.: 2021-01

Fecha de publicación: 11/01/2021

Tema: Vulnerabilidad en la herramienta de administración Microsoft Windows PsExec.

Versiones afectadas:

Todas las versiones existentes de Microsoft Windows PsExec, en múltiples versiones de Windows desde Windows XP hasta Windows 10.

Descripción

Un investigador de seguridad, ha descubierto una vulnerabilidad en la utilidad Microsoft Windows PsExec. Esta vulnerabilidad permitiría a un atacante local realizar una escalada de privilegios. Según el CEO y cofundador de 0patch, Mitja Kolsek: Cualquier computadora con Windows donde “los administradores ejecuten de forma remota el uso de PsExec (o herramientas de administración que utilizan PsExec) si la máquina ya tiene un atacante que no es administrador tratando de elevar sus privilegios” es vulnerable a los ataques que intentan explotar esta vulnerabilidad.

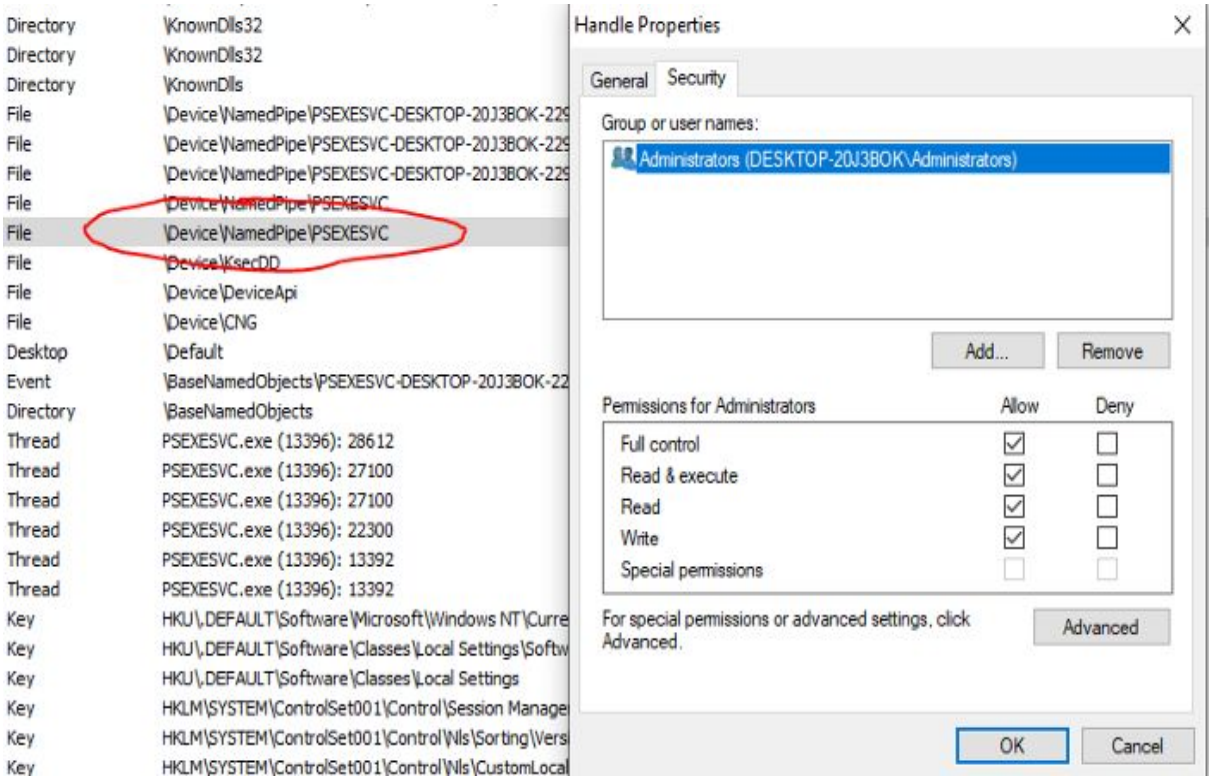
PsExec es un reemplazo de telnet totalmente interactivo que permite a los administradores del sistema ejecutar programas en sistemas remotos. La herramienta PsExec también está integrada y utilizada por herramientas empresariales para iniciar ejecutables de forma remota en otras computadoras.

Para que la herramienta funcione, se lanza el recurso *psexesvc* con privilegios de administrador en la máquina remota, está usa una extensión conocida como ‘NamedPipes’ para la comunicación con el ejecutable *psexec.exe*, que son las que interpretarán los comandos que se ejecutarán.

La vulnerabilidad encontrada está en que cualquier otro programa sin privilegios puede crear **Named Pipes** con el mismo nombre antes que **psexec**, al no comprobar que programa ha creado el "pipe", este sería capaz de suplantar el "pipe" y poder escalar privilegios en el sistema.

PsExec contiene un recurso integrado llamado **"PSEXESVC"**, que es el componente a nivel de servicio ejecutable que se extrae, copia y ejecuta en una máquina remota como SYSTEM siempre que se ejecuta PsExec en un cliente apuntando a una máquina remota. La comunicación entre el cliente PsExec y el servicio PSEXESVC remoto tiene lugar a través de canalizaciones con nombre. Específicamente, la pipe denominada "\ PSEXESVC" es responsable de analizar y ejecutar los comandos del cliente PsExec, como "qué aplicación ejecutar", "datos de línea de comandos relevantes", etc.

Por razones de seguridad, la canalización **"\ PSEXESVC"** del servicio **PSEXESVC** está protegida y solo permite a los administradores acceso de lectura / escritura, evitando así que los usuarios locales con pocos privilegios lean / escriban en la canalización del servicio.

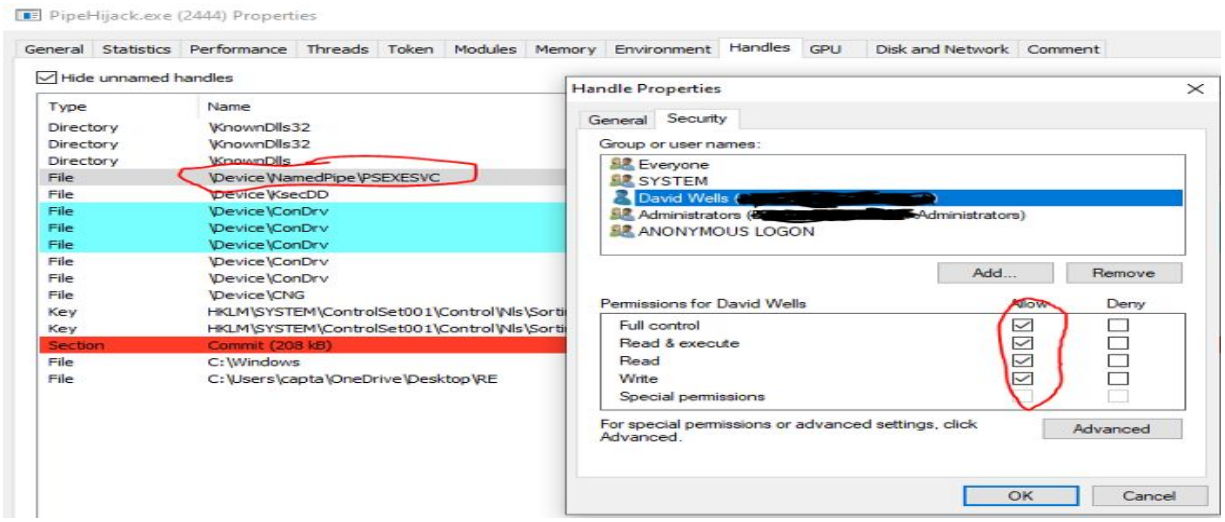


Sin embargo, a través de la colocación en cuclillas de la pipe ***(un método en el que se crea el pipe primero)***, es posible que una aplicación con pocos privilegios obtenga acceso a esta pipe. Si una aplicación local con pocos privilegios crea el pipe con nombre **"\ PSEXESVC"** antes de que se ejecute PSEXESVC, entonces PSEXESVC obtendrá un identificador para la instancia existente en lugar de crear el pipe con nombre, lo que tendrá algunas consecuencias inesperadas, como se describe más adelante.

```
loc_4038C3:
lea     eax, [ebp+SecurityAttributes]
push    eax             ; lpSecurityAttributes
push    2710h           ; nDefaultTimeOut
push    10000h          ; nInBufferSize
push    10000h          ; nOutBufferSize
push    0FFh            ; nMaxInstances: PIPE_UNLIMITED_INSTANCES
push    6               ; dwPipeMode: PIPE_READMODE_MESSAGE | PIPE_TYPE_MESSAGE
push    3               ; openMode: PIPE_ACCESS_DUPLEX
lea     eax, [ebp+Name]
push    eax             ; lpName: "\\\\.\pipe\PSEXECSVC"
call    ds:CreateNamedPipeW
push    0               ; dwFlags
```

Se puede observar el argumento **nMaxInstances** , que permite que existan instancias de pipe ***"\ PSEXESVC"*** ilimitadas. La misma no asegura que sea la primera aplicación en crear el pipe ***"\ PSEXESVC"***, lo que normalmente se hace usando la bandera **FILE_FLAG_FIRST_PIPE_INSTANCE** . Se crea el pipe con un nombre existente, simplemente para que obtenga un identificador para el pipe ***"\ PSEXESVC"*** existente después de la llamada. Esto terminará heredando la ACL del pipe existente en lugar de aplicar su propia ACL "Solo administradores" al pipe, independientemente del hecho de que los atributos de seguridad digan lo contrario en su llamada *"CreateNamedPipe"* .

En el siguiente ejemplo se muestra un programa simple "PipeHijack.exe" que crea esta el pipe "\ PSEXESVC" con acceso de lectura / escritura disponible para: "David Wells", un usuario no elevado.



Impacto

Con esta ejecución, si alguna vez PsExec se ejecuta local o remotamente en la máquina afectada, la instancia de PSEXESVC obtendrá un identificador para el pipe, en la que, se obtendrá privilegios para leer / escribir, lo que permitirá que la aplicación con pocos privilegios se comunique con este servicio del SISTEMA PSEXESVC!.

Al interactuar con el servicio PSEXESVC, se podría realizar ingeniería inversa del protocolo PSEXESVC, imitando al cliente PsExec del que cree que recibe comandos, por lo que cualquier usuario podría ejecutar cualquier proceso como SYSTEM.

Solución y prevención

- Aplicar de forma inmediata el parche de seguridad PsExec v2.21, su versión más reciente: ***ACTUALIZAR*.**

Información adicional

- https://medium.com/tenable-techblog/psexec-local-privilege-escalation-2e8069adc9c8
- https://docs.microsoft.com/en-us/sysinternals/downloads/psexec
- https://unaaldia.hispasec.com/2020/12/escalado-de-privilegios-sin-parchear-en-psexec.html