Error de verificación de inicio de sesión previo de CSD de HostScan en Secure Client

Contenido

Problema

Un usuario encuentra el mensaje de error "Error en la verificación de inicio de sesión previo de CSD de HostScan" cuando intenta conectarse a una VPN mediante Cisco Secure Client en un dispositivo con Windows 11. El error se produce antes de que se muestre el mensaje de inicio de sesión, lo que impide que el usuario acceda a la conexión VPN. El mismo usuario puede conectarse correctamente a la VPN desde otro dispositivo utilizando credenciales y perfiles VPN idénticos, lo que indica que el problema es específico del dispositivo en lugar de relacionado con las credenciales.

Las entradas adicionales del registro de errores observadas incluyen:

- CONNECTIFC_ERROR_FILE_OPEN_FAILED (Código devuelto: -30015466 / 0xFE360016)
- Error de procesamiento de HostScan
- No se pudo establecer la conexión debido a un problema de red o de PC

El usuario pudo conectarse a otros perfiles VPN en los que no se habilitó el estado, pero no pudo conectarse a perfiles en los que sí se habilitó el estado. La instalación funcionaba anteriormente sin que se produjeran cambios conocidos en la configuración.

Entorno

- Cisco Secure Client versión 5.1.7.80
- Sistema operativo: Windows 11
- Perfil VPN con el estado habilitado

- El problema es específico del dispositivo y afecta solo a un usuario en un dispositivo en particular
- Relacionado con la ID de bug de Cisco: CSCwk54713

Resolución

La resolución implica realizar una desinstalación completa y limpia de Cisco Secure Client y reinstalar el software. Los métodos estándar de desinstalación y reinstalación no siempre resuelven el problema debido a entradas del Registro dañadas o archivos residuales.

Paso 1: Desactivar servicios de terceros

Deshabilite todos los servicios de terceros en Msconfig, incluidos los servicios proxy si están disponibles, y mantenga activos únicamente los módulos de Cisco Secure Client.

Paso 2: Limpiar la desinstalación con la herramienta Microsoft

Utilice la herramienta Solucionador de problemas de instalación y desinstalación de programas de Microsoft para quitar todos los módulos de Cisco del dispositivo afectado. Esta herramienta proporciona una desinstalación más completa que los métodos de desinstalación estándar de Windows.

Solucione los problemas que bloquean la instalación o eliminación de programas.

Paso 3: Limpieza manual de archivos

Después de la desinstalación, compruebe manualmente y elimine cualquier carpeta, archivo ejecutable, archivo DLL de Cisco restante de estos directorios:

```
C:\Program Files (x86)\Cisco
C:\ProgramData\Cisco\
```

```
C:\Users\<current user>\AppData\Local\Cisco
```

Elimine los archivos y carpetas residuales que se encuentren en estas ubicaciones, ya que no siempre permanecen incluso después del proceso de desinstalación.

Paso 4: Limpieza del Registro

Verifique las trayectorias de este registro para cualquier entrada antigua de Cisco Secure Client y retírelas si existen:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco
HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco
```

Paso 5: Habilitar registro de depuración (opcional)

Si se necesita más resolución de problemas, habilite el registro Curl copiando el archivo debuglogconfig.json:

```
{
"web_helper" : 3,
"vpn_ipsec_ikev2" : 3,
"vpn_curl" : 3,
"vpn_state" : 3
}
```

en este directorio:

```
C:\ProgramData\Cisco\Cisco Secure Client
```

Paso 6: Reinicio del sistema

Reinicie el extremo para asegurarse de que todos los cambios surtan efecto y borre los procesos o bloqueos del Registro restantes.

Paso 7: Reinstalar Cisco Secure Client

Instale el paquete de preimplementación de Cisco Secure Client o permita la instalación automática a través de herramientas de administración como Intune. Verifique que la instalación se haya realizado correctamente antes de continuar.

Paso 8: Probar conexión VPN

Intento de conexión con el perfil VPN que había fallado anteriormente. Si el problema persiste, genere un nuevo paquete DART para analizarlo más a fondo.

⚠ Precaución: Posible. Los detalles mencionados aquí parecen contener procedimientos o comandos que podrían causar un impacto significativo si se ejecutan. Asegúrese de que estos procedimientos o comandos han sido evaluados por una PYME o una unidad empresarial antes de ejecutarlos o recomendarlos.

Causa

El problema es causado por entradas de registro dañadas o interferencias de software de terceros que impide que las bibliotecas y ejecuciones de Hostscan se inicien o actualicen correctamente. Esta corrupción afecta al proceso de verificación previa al inicio de sesión de CSD (Cisco Security Desktop), que es necesario para los perfiles VPN con el estado habilitado. La corrupción suele producirse en el nivel del dispositivo, lo que explica por qué el mismo usuario puede conectarse correctamente desde otros dispositivos. Los métodos de desinstalación estándar no siempre quitan todos los componentes dañados, lo que requiere la limpieza manual de archivos y entradas del Registro.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).