

Base de datos de firmas de Windows Defender vacía después de que la desinstalación de Norton Antivirus provoque un error de estado de ISE

Contenido

Problema

Los terminales Windows 11 25H2 que se conectan a través de VPN no superan las comprobaciones de estado de ISE y se marcan como no conformes, lo que impide la autenticación y el acceso a los recursos de red. El terminal cumple los requisitos de la regla ISE, pero sigue informando de que el usuario no cumple los requisitos después de la conexión VPN.

La comprobación de estado falla específicamente para la validación de la versión de definición de antivirus de Windows Defender con este error:

```
[csc_iseposture]Function: CheckOpswat::CheckOpswatProd Thread Id: 0x277C File: CheckOpswat.cpp Line: 27
```

El agente de estado informa de que Windows Defender tiene una versión de definición vacía y una fecha de definición de 0, lo que provoca un error en el requisito AUC_WIN11_IT.

Entorno

- Identity Services Engine (ISE) 3.3
- Terminales Windows 11 25H2
- Módulo Cisco Secure Client con estado de ISE
- ISEComcompliance module versión 4.3.5626.8192

- Windows Defender versión 4.18.25080.5
- Anteriormente tenía instalado y desinstalado el antivirus Norton 360
- Conexión VPN con aplicación de estado ISE habilitada

Resolución

La resolución implica desinstalar Norton y, a continuación, actualizar manualmente las firmas de Windows Defender y comprender el comportamiento de coexistencia entre el antivirus de terceros y Windows Defender.

Paso 1: Actualizar firmas de Windows Defender

1.- Navegue hasta la configuración de Seguridad de Windows y actualice manualmente la base de datos de firmas:

2.- Vaya a Configuración → Privacidad y seguridad → Seguridad de Windows → Protección frente a virus y amenazas → Actualizaciones de protección frente a virus y amenazas → Buscar actualizaciones.

3.- Espere hasta que la versión de inteligencia de seguridad muestre un valor no vacío y una marca de tiempo actual antes de proceder con la validación de estado.

Paso 3: Verificar cumplimiento de estado

Después de actualizar las firmas, vuelva a conectarse a la VPN y verifique que se supere la comprobación de estado. La versión de inteligencia de seguridad debe mostrar ahora un valor válido en lugar de estar vacía.

Consideraciones importantes para los antivirus de terceros

Cuando se instala un antivirus de terceros y se registra correctamente en el Centro de seguridad de Windows, Microsoft Windows pone intencionadamente Windows Defender en modo pasivo para evitar conflictos. En el modo pasivo, Defender no publica sus datos de actualización de firmas a través del Centro de seguridad de Windows/API WMI que lee OPSWAT, lo que provoca errores en las comprobaciones de estado.

Para evitar este problema, desinstale la aplicación de terceros que Windows pone en modo activo. Si es necesario volver a instalar Norton u otro software antivirus de terceros, tenga en cuenta que esto hace que el terminal vuelva a ser no conforme.

Causa

La causa principal es que la base de datos de firmas de Windows Defender se queda obsoleta cuando un antivirus de terceros (Norton) es la solución antivirus principal. Mientras se instaló Norton, Windows intencionadamente mantuvo obsoleto el almacén de definiciones de Defender porque el software antivirus de modo pasivo no recibe actualizaciones programadas. Después de desinstalar Norton, Windows Defender se convirtió en el antivirus principal, pero su base de datos de firmas permaneció vacía porque la primera extracción de firma se coloca en la cola detrás de Windows Update y solo se ejecuta automáticamente en su siguiente desencadenador programado o cuando el usuario la fuerza manualmente.

El método SDK de OPSWAT v4 1001 (GetDefinitionState) devuelve una carga vacía cuando el almacén de definiciones locales de Defender está vacío, lo que hace que el agente de estado de ISE transmita una versión de definición vacía a ISE. A continuación, ISE compara este valor vacío con el umbral de la política y marca el terminal como no conforme.

Contenido relacionado

- [Guía para administradores de Cisco Secure Client - Consideraciones sobre el software de terceros](#)
- [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).