

Banco de dados de assinatura do Windows Defender vazio depois que a desinstalação do Norton Antivirus causa falha de postura do ISE

Contents

Problema

Os pontos finais do Windows 11 25H2 que se conectam por VPN não passam nas verificações de postura do ISE e são marcados como não compatíveis, impedindo a autenticação e o acesso aos recursos da rede. O endpoint atende aos requisitos da regra do ISE, mas ainda relata "usuário não atende aos requisitos" após a conexão VPN.

A verificação de postura falha especificamente na validação da versão da definição de antivírus do Windows Defender com este erro:

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

O agente de postura relata que o Windows Defender tem uma versão de definição vazia e uma data de definição igual a 0, causando a falha do requisito AUC_WIN11_IT.

Ambiente

- Identity Services Engine (ISE) 3.3
- Pontos de extremidade do Windows 11 25H2
- Cisco Secure Client com módulo de postura do ISE
- Módulo de conformidade ISEC versão 4.3.5626.8192
- Windows Defender versão 4.18.25080.5

- Anteriormente, o antivírus Norton 360 estava instalado e desinstalado
- Conexão VPN com imposição de postura do ISE habilitada

Resolução

A resolução envolve a desinstalação do Norton e a atualização manual das assinaturas do Windows Defender e a compreensão do comportamento de coexistência entre o antivírus de terceiros e o Windows Defender.

Passo 1: Atualizar Assinaturas do Windows Defender

1.- Navegue até as configurações de Segurança do Windows e atualize manualmente o banco de dados de assinaturas:

2.- Vá para Configurações → Privacidade e segurança → Segurança do Windows → Proteção contra vírus e ameaças → Atualizações de proteção contra vírus e ameaças → Verificar se há atualizações.

3.- Espere até que a versão de inteligência de segurança mostre um valor não vazio e um carimbo de data/hora atual antes de continuar com a validação da postura.

Passo 3: Verificar conformidade com postura

Depois de atualizar as assinaturas, reconecte-se à VPN e verifique se a verificação de postura foi bem-sucedida. A versão da inteligência de segurança agora deve exibir um valor válido em vez de ficar vazia.

Considerações importantes sobre antivírus de terceiros

Quando qualquer antivírus de terceiros é instalado e registrado corretamente no Windows Security Center, o Microsoft Windows coloca intencionalmente o Windows Defender no modo

passivo para evitar conflitos. No modo passivo, o Defender não publica seus dados de atualização de assinatura por meio da API do Windows Security Center/WMI lida pelo OPSWAT, o que causa falha nas verificações de postura.

Para evitar esse problema, desinstale o aplicativo de terceiros que o Windows coloca no modo Ativo. Se for necessário reinstalar o Norton ou outro software antivírus de terceiros, lembre-se de que isso fará com que o endpoint se torne não compatível novamente.

Causa

A causa principal é que o banco de dados de assinaturas do Windows Defender se torna obsoleto quando um antivírus de terceiros (Norton) é a principal solução antivírus. Enquanto o Norton estava instalado, o Windows intencionalmente manteve o armazenamento de definições do Defender obsoleto porque o software antivírus de modo passivo não recebe atualizações programadas. Depois que o Norton foi desinstalado, o Windows Defender se tornou o antivírus principal, mas seu banco de dados de assinaturas permaneceu vazio porque o primeiro recebimento de assinaturas é enfileirado atrás do Windows Update e só é executado automaticamente no próximo disparador agendado ou quando forçado manualmente pelo usuário.

O método SDK do OPSWAT v4 1001 (GetDefinitionState) retorna uma carga vazia quando o repositório de definições locais do Defender está vazio, fazendo com que o agente de postura do ISE transmita uma versão de definição vazia para o ISE. Em seguida, o ISE compara esse valor vazio com o limite da política e marca o endpoint como não compatível.

Conteúdo relacionado

- [Guia do administrador do Cisco Secure Client - Considerações sobre software de terceiros](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.