

Il database delle firme di Windows Defender è vuoto dopo la disinstallazione di Norton Antivirus causa un errore di postura ISE

Sommario

Problema

Gli endpoint Windows 11 25H2 che si connettono tramite VPN non superano i controlli di postura ISE e sono contrassegnati come non conformi, impedendo l'autenticazione e l'accesso alle risorse di rete. L'endpoint soddisfa i requisiti della regola ISE, ma segnala comunque "l'utente non soddisfa i requisiti" dopo la connessione VPN.

Il controllo della postura non riesce in modo specifico per la convalida della versione della definizione antivirus di Windows Defender con questo errore:

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

L'agente di postura segnala che Windows Defender ha una versione di definizione vuota e una data di definizione pari a 0, causando l'esito negativo del requisito AUC_WIN11_IT.

Ambiente

- Identity Services Engine (ISE) 3.3
- Endpoint Windows 11-25H2
- Cisco Secure Client con modulo ISE Posture
- Modulo ISECompliance versione 4.3.5626.8192
- Windows Defender versione 4.18.25080.5

- In precedenza, Norton 360 antivirus era installato e disinstallato
- Connessione VPN con imposizione postura ISE abilitata

Risoluzione

La risoluzione prevede la disinstallazione di Norton, quindi l'aggiornamento manuale delle firme di Windows Defender e la comprensione del comportamento di coesistenza tra antivirus di terze parti e Windows Defender.

Passaggio 1: Aggiorna firme di Windows Defender

1.- Passare alle impostazioni di protezione di Windows e aggiornare manualmente il database delle firme:

2.- Andare a Impostazioni → Privacy e sicurezza → Sicurezza di Windows → Protezione da virus e minacce → Aggiornamenti per la protezione da virus e minacce → Verificare la disponibilità di aggiornamenti.

3.- Attendere che la versione di Security Intelligence visualizzi un valore non vuoto e un timestamp corrente prima di procedere con la convalida della postura.

Passaggio 3: Verifica conformità postura

Dopo aver aggiornato le firme, riconnettersi alla VPN e verificare che il controllo della postura abbia esito positivo. La versione dell'intelligence di sicurezza deve ora visualizzare un valore valido anziché essere vuota.

Considerazioni importanti per l'antivirus di terze parti

Quando un programma antivirus di terze parti è installato e correttamente registrato in Centro sicurezza PC Windows, Microsoft Windows attiva intenzionalmente Windows Defender in modalità

passiva per evitare conflitti. In modalità passiva, Defender non pubblica i dati di aggiornamento della firma tramite l'API Centro sicurezza PC Windows/WMI letta da OPSWAT, pertanto i controlli della postura non riescono.

Per evitare questo problema, disinstallare l'applicazione di terze parti attivata da Windows in modalità attiva. Se è necessario reinstallare Norton o un altro software antivirus di terze parti, tenere presente che in questo modo l'endpoint diventa nuovamente non conforme.

Causa

La causa principale è che il database delle firme di Windows Defender diventa obsoleto quando un antivirus di terze parti (Norton) è la soluzione antivirus principale. Durante l'installazione di Norton, Windows ha intenzionalmente mantenuto l'archivio delle definizioni di Defender non aggiornato perché il software antivirus in modalità passiva non riceve aggiornamenti pianificati. Dopo la disinstallazione di Norton, Windows Defender è diventato l'antivirus principale, ma il relativo database delle firme è rimasto vuoto perché il primo pull di firma viene accodato dietro Windows Update e viene eseguito automaticamente solo al successivo trigger pianificato o quando viene forzato manualmente dall'utente.

Il metodo 1001 (GetDefinitionState) di OPSWAT v4 SDK restituisce un payload vuoto quando l'archivio delle definizioni locali di Defender è vuoto, pertanto l'agente di postura ISE trasmette una versione di definizione vuota ad ISE. ISE confronta quindi questo valore vuoto con la soglia dei criteri e contrassegna l'endpoint come non conforme.

Contenuto correlato

- [Guida per l'amministratore di Cisco Secure Client - Considerazioni sul software di terze parti](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).