

Windows Defender Handtekening Database leeg na Norton Antivirus verwijderen veroorzaakt ISE houding falen

Inhoud

uitgifte

Windows 11 25H2-eindpunten die verbinding maken via VPN mislukken ISE-houdingscontroles en zijn gemarkeerd als niet-conform, waardoor verificatie en toegang tot netwerkbronnen wordt voorkomen. Het eindpunt voldoet aan de ISE-regelvereisten, maar rapporteert na de VPN-verbinding nog steeds "gebruiker die niet aan de vereiste voldoet".

De controle van de houding mislukt specifiek voor de validatie van de antivirusdefinitie van Windows Defender met deze fout:

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

De houdingsagent meldt dat Windows Defender een lege definitieversie en definitiedatum van 0 heeft, waardoor de AUC_WIN11_IT-vereiste mislukt.

milieu

- Identity Services Engine (ISE) 3.3
- Windows 11 25H2-eindpunten
- Cisco Secure Client met ISE Posture-module
- ISECompliance module versie 4.3.5626.8192
- Windows Defender versie 4.18.25080.5

- Eerder had Norton 360 antivirus geïnstalleerd en verwijderd
- VPN-verbinding met ISE-postuur ingeschakeld

resolutie

De oplossing bestaat uit het verwijderen van Norton, het handmatig bijwerken van Windows Defender-handtekeningen en het begrijpen van het coëxistentiegedrag tussen antivirus van derden en Windows Defender.

Stap 1: Windows Defender-handtekeningen bijwerken

- 1.- Navigeer naar de beveiligingsinstellingen van Windows en werk de handtekeningendatabase handmatig bij:
- 2.- Ga naar Instellingen → Privacy en beveiliging → Windows Security → Virus- en bedreigingsbescherming → Virus- en bedreigingsbeschermingsupdates → Controleer op updates.
- 3.- Wacht tot de versie van de beveiligingsinformatie een niet-lege waarde en een huidige tijdstempel toont voordat u doorgaat met de validatie van de houding.

Stap 3: Controleren of de houding voldoet

Nadat u de handtekeningen hebt bijgewerkt, maakt u opnieuw verbinding met de VPN en controleert u of de houdingscontrole is geslaagd. De versie van de beveiligingsinformatie moet nu een geldige waarde weergeven in plaats van leeg te zijn.

Belangrijke overwegingen voor antivirus van derden

Wanneer een antivirus van derden is geïnstalleerd en correct is geregistreerd bij Windows Security Center, zet Microsoft Windows Defender opzettelijk in de passieve modus om conflicten te voorkomen. In de passieve modus publiceert Defender zijn handtekeningversheidsgegevens

niet via de Windows Security Center/WMI API die OPSWAT leest, waardoor de houdingscontroles mislukken.

Om dit probleem te voorkomen, verwijdt u de toepassing van de derde partij die door Windows in de actieve modus wordt geplaatst. Als het opnieuw installeren van Norton of andere antivirussoftware van derden vereist is, moet u zich ervan bewust zijn dat dit ervoor zorgt dat het eindpunt weer niet-conform wordt.

Oorzaak

De hoofdoorzaak is dat de Windows Defender-handtekeningendatabase muf wordt wanneer een antivirusoplossing van derden (Norton) de primaire antivirusoplossing is. Terwijl Norton was geïnstalleerd, hield Windows opzettelijk de Defender-definities-winkel stabiel omdat antivirussoftware in de passieve modus geen geplande updates ontvangt. Nadat Norton was verwijderd, werd Windows Defender de primaire antivirus, maar de database met handtekeningen bleef leeg omdat de eerste handtekening aantrekking achter Windows Update in de wachtrij staat en alleen automatisch wordt uitgevoerd op de volgende geplande trigger of wanneer handmatig door de gebruiker wordt gedwongen.

De OPSWAT v4 SDK-methode 1001 (GetDefinitionState) retourneert een lege payload wanneer de Defender local definitions store leeg is, waardoor de ISE posture agent een lege definitieversie naar ISE verzendt. ISE vergelijkt deze lege waarde vervolgens met de beleidsdrempel en markeert het eindpunt als niet-conform.

Gerelateerde inhoud

- [Cisco Secure Client Administrator Guide - Overwegingen van derden met betrekking tot software](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.