

Die Signaturdatenbank von Windows Defender ist leer, nachdem die Deinstallation von Norton Antivirus einen ISE-Statusfehler verursacht hat.

Inhalt

Problem

Die ISE-Statusprüfungen für Windows 11/25H2-Endgeräte, die über VPN eine Verbindung herstellen, sind fehlgeschlagen. Sie werden als nicht kompatibel markiert, wodurch die Authentifizierung und der Zugriff auf Netzwerkressourcen verhindert werden. Das Endgerät erfüllt die ISE-Regelanforderungen, meldet jedoch nach der VPN-Verbindung "Benutzer erfüllt Anforderung nicht".

Die Statusprüfung schlägt bei der Überprüfung der Version der Windows Defender-Antivirendefinition mit folgendem Fehler fehl:

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

Der Status-Agent meldet, dass Windows Defender über eine leere Definitionsversion und ein leeres Definitionsdatum von 0 verfügt, was dazu führt, dass die Anforderung von AUC_WIN11_IT fehlschlägt.

Umwelt

- Identity Services Engine (ISE) 3.3
- Windows 11 25H2-Endgeräte
- Cisco Secure Client mit ISE Posture-Modul
- ISECompliance-Modul Version 4.3.5626.8192

- Windows Defender Version 4.18.25080.5
- Norton 360 Antivirus bereits installiert und deinstalliert
- VPN-Verbindung mit aktivierter ISE-Statusdurchsetzung

Auflösung

Die Lösung besteht darin, Norton zu deinstallieren, dann manuell die Windows Defender-Signaturen zu aktualisieren und das Koexistenzverhalten zwischen Antivirus-Software von Drittanbietern und Windows Defender zu verstehen.

Schritt 1: Windows Defender-Signaturen aktualisieren

1.- Navigieren Sie zu den Windows-Sicherheitseinstellungen, und aktualisieren Sie die Signaturdatenbank manuell:

2.- Gehen Sie zu Einstellungen → Datenschutz & Sicherheit → Windows-Sicherheit → Viren- & Bedrohungsschutz → Viren- & Bedrohungsschutz-Updates → Nach Updates suchen.

3.- Warten Sie, bis die Version der Sicherheitsinformationen einen nicht leeren Wert und einen aktuellen Zeitstempel anzeigt, bevor Sie mit der Statusüberprüfung fortfahren.

Schritt 3: Überprüfung der Einhaltung von Statusrichtlinien

Stellen Sie nach der Aktualisierung der Signaturen erneut eine Verbindung mit dem VPN her, und vergewissern Sie sich, dass die Statusüberprüfung erfolgreich verläuft. Die Version der Sicherheitsinformationen muss jetzt einen gültigen Wert anzeigen, anstatt leer zu sein.

Wichtige Überlegungen zum Virenschutz von Drittanbietern

Wenn Antivirenprogramme von Drittanbietern installiert und ordnungsgemäß im Windows-

Sicherheitscenter registriert sind, versetzt Microsoft Windows Defender absichtlich in den passiven Modus, um Konflikte zu vermeiden. Im passiven Modus veröffentlicht Defender seine Signaturaktualisierungsdaten nicht über die von OPSWAT eingelesene Windows-Sicherheitscenter/WMI-API, sodass Statusüberprüfungen fehlschlagen.

Um dieses Problem zu vermeiden, deinstallieren Sie die Anwendung eines Drittanbieters, die Windows in den aktiven Modus versetzt. Wenn eine Neuinstallation von Norton oder anderer Antiviren-Software von Drittanbietern erforderlich ist, beachten Sie, dass das Endgerät dadurch wieder nicht mehr kompatibel ist.

Ursache

Die Ursache liegt darin, dass die Windows Defender-Signaturdatenbank veraltet ist, wenn ein Antivirus-Programm eines Drittanbieters (Norton) die primäre Antivirus-Lösung ist. Während der Installation von Norton hielt Windows den Defender-Definitionsspeicher absichtlich veraltet, da die Antivirus-Software im passiven Modus keine geplanten Updates erhält. Nachdem Norton deinstalliert wurde, wurde Windows Defender zum primären Antivirus-Programm, die Signaturdatenbank blieb jedoch leer, da das erste Signaturabruf-Paket hinter Windows Update in die Warteschlange gestellt wurde und nur automatisch auf dem nächsten geplanten Trigger ausgeführt wird, oder wenn der Benutzer es manuell erzwingt.

Die OPSWAT v4 SDK-Methode 1001 (GetDefinitionState) gibt eine leere Nutzlast zurück, wenn der lokale Defender-Definitionsspeicher leer ist, was dazu führt, dass der ISE-Statusagent eine leere Definitionsversion an ISE sendet. Die ISE vergleicht diesen leeren Wert mit dem Richtlinienschwellenwert und markiert den Endpunkt als nicht konform.

Verwandte Inhalte

- [Administratoranleitung für Cisco Secure Client - Überlegungen zu Drittanbietersoftware](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.