

AnyConnect VPN-Zugriff für sichere Clients aufgrund von Compliance-Problemen mit dem Endpunkt-Sicherheitsstatus verweigert

Inhalt

Problem

Mehrere Benutzer können keine Verbindung zu AnyConnect VPN und ZTA (Zero Trust Access) herstellen und erhalten die Fehlermeldung "Login denied" (Anmeldung abgelehnt). Ihre Umgebung erfüllt nicht die von Ihrem Administrator definierten Zugriffskriterien."

Das Problem bezieht sich auf die Endpunktstatus-Compliance, bei der die Endpunktsicherheits-Agent-Anforderung als nicht übereinstimmend gemeldet wird. Benutzer haben VPN- und ZTA-Zugriffsverweigerungen, wenn sie versuchen, eine Verbindung über den Cisco Secure Client herzustellen.

Die Statusüberprüfung zeigt, dass der Trellix Endpoint Security-Status auf betroffenen Endgeräten fehlschlägt und eine erfolgreiche Authentifizierung beim VPN-Service verhindert.

Umwelt

- Cisco Secure Client (AnyConnect und Zero Trust Access)
- Trellix Endpoint Security Agent Version 5.8.4.505
- VPN-Statusprofil: KFIN_SECURE_VPN mit Endpunkt-Durchsetzung von Sicherheitsagenten
- Statusanforderung: Endpoint Security Agent mit Updates innerhalb der letzten 14 Tage
- Windows-Endpunkte mit Ausführung des Trellix Agent Service
- Umbrella Agent-Prozesse auf Endpunkten erkannt

Auflösung

Das Problem wurde durch die Behebung der Compliance-Probleme mit dem Status des Trellix Endpoint Security-Agenten behoben. Die in den nächsten Abschnitten beschriebenen Schritte zur Fehlerbehebung wurden implementiert.

Schritt 1: Konfiguration des Statusprofils überprüfen

Überprüfen Sie das VPN-Statusprofil, um die Anforderungen der Sicherheitsagenten für Endgeräte zu bestätigen. Das KFIN_SECURE_VPN-Profil erzwingt, dass ein Endpunkt-Sicherheits-Agent innerhalb der letzten 14 Tage ausgeführt und aktualisiert werden muss.

Phase 2: Sicherheitsstatus für Trellix-Endpunkte überprüfen

Überprüfen Sie den aktuellen Status des Trellix Endpoint Security-Agenten auf betroffenen Endgeräten:

```
Trellix Agent Service: masvc.exe  
Version: 5.8.4.505  
Install Location: C:\Program Files\McAfee\Agent\  
Display Name: Trellix Agent  
Publisher: Trellix
```

Schritt 3: Neuinstallation von Trellix Endpoint Security

Führen Sie eine vollständige Neuinstallation von Trellix Endpoint Security auf betroffenen Endgeräten durch:

1. Deinstallieren Sie den vorhandenen Trellix Endpoint Security Agent vollständig.
2. Starten Sie das System neu.

3. Installieren Sie die neueste genehmigte Version des Trellix-Agenten gemäß den Unternehmensstandards.
4. Stellen Sie sicher, dass der Agent nach der Installation erfolgreich ausgeführt wird.
5. Bestätigen Sie, dass die Signatur-/Inhaltsaktualisierungen erfolgreich abgeschlossen wurden.

Schritt 4: Aktivieren von TRACE-Protokollierung für Cisco Secure Client (ZTA)

Aktivieren Sie eine detaillierte Protokollierung, um Statusüberprüfungsdetails zu erfassen.

Erstellen Sie die Datei "logconfig.json" mit folgendem Inhalt:

```
{ "global": "DBG_TRACE" }
```

Speichern Sie die Datei im entsprechenden Verzeichnis:

- Windows: C:\ProgramData\Cisco\Cisco Sicherer Client\ZTA
- MacOS: /opt/cisco/secureclient/zta

Starten Sie den Cisco Secure Client/ZTA-Dienst neu, nachdem Sie die Datei erstellt haben.

Schritt 5: Sammeln aktualisierter DART-Pakete

Nach der Implementierung der Änderungen sollten Sie ein neues DART-Paket zusammenstellen, um die Auflösung zu validieren und die korrekte Erkennung des Sicherheitsstatus zu bestätigen.

Ursache

Die Ursache wurde als Trellix Endpoint Security-Agent-Compliance-Probleme identifiziert. Für das

VPN-Statusprofil musste in den letzten 14 Tagen ein Security Agent für Endgeräte mit Updates ausgeführt werden, der Trellix Endpoint Security Agent erfüllte diese Compliance-Kriterien jedoch nicht. Das Statusbewertungsmodul konnte den Status des Sicherheitsagenten des Endpunkts nicht richtig erkennen oder validieren, was zu einer Zugriffsverweigerung für VPN- und ZTA-Verbindungen führte. Das Problem bezog sich speziell auf die Trellix-Agentenkonfiguration und erforderte das Eingreifen des Trellix-Supportteams, um die zugrunde liegenden Probleme mit der Agentenkonformität zu beheben.

Verwandte Inhalte

- [Sammeln detaillierter ZTNA-Protokolle zur Fehlerbehebung](#)
- [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.