

Umbrella-Modul bleibt auf sicherem Client deaktiviert

Inhalt

Problem

Das Umbrella DNS Security-Modul im Cisco Secure Client (AnyConnect VPN Agent) bleibt nach Anwendung der Umbrella-Profildatei aufgrund einer fehlenden Übereinstimmung der Fingerabdrücke bei der Geräteregistrierung im Status "Disabled" (Deaktiviert). Dieses Problem besteht in verschiedenen Netzwerkimplementierungen fort, einschließlich der Verbindungen in der Hauptniederlassung und über den persönlichen Hotspot.

Diagnoseartefakte wie Screenshots, DART-Paketerfassungen und Paketerfassungsdateien weisen auf Fehler bei der Geräteregistrierung hin, die auf eine falsche Fingerabdruckübereinstimmung in der Datei OrgInfo.json zurückzuführen sind:

- Das Umbrella-Modul zeigt den Status "Deaktiviert" an.
- Das Problem tritt nach der Anwendung der Umbrella-Profildatei auf.
- Das Problem tritt bei mehreren Netzwerken auf.
- Diagnoseprotokolle und Paketerfassungen zeigen Fehler bei der Geräteregistrierung an.

Umwelt

- Produkt: Cisco Secure Client (AnyConnect VPN Agent) mit Umbrella-Modul
- Plattform: Windows-Betriebssystem
- Umbrella DNS Security-Funktion
- Umbrella-Profildatei und involvierte OrgInfo.json
- Netzwerkimplementierungen: Büro, persönlicher Hotspot
- Diagnostische Artefakte: DART-Paket, Paketerfassung, Screenshot
- Software-Version: Alle

Auflösung

Dieser detaillierte Workflow löst den Status "Deaktiviert" des Umbrella-Moduls auf, indem die Fingerabdruck-Diskrepanz in der Datei OrgInfo.json korrigiert und das Gerät beim Umbrella-Cloud-Service neu registriert wird.

Laden Sie die Datei New OrgInfo.json aus dem SSE Dashboard herunter.

So stellen Sie sicher, dass bei der Geräteregistrierung der richtige Fingerabdruck verwendet wird:

1. Holen Sie sich eine neue OrgInfo.json-Datei.
2. Laden Sie die aktualisierte Datei OrgInfo.json direkt vom Cisco Secure Service Edge (SSE)-Dashboard herunter.

Stoppen des Cisco Secure Client - AnyConnect VPN Agent Service

Um den Dienst anzuhalten, müssen die dem Umbrella-Modul zugeordneten Dateien sicher geändert werden:

Öffnen Sie Windows Services, und beenden Sie den Dienst mit dem Namen Cisco Secure Client - AnyConnect VPN Agent.

Löschen Sie alle Inhalte aus dem Umbrella Module-Ordner

1. Löschen Sie alle potenziell beschädigten oder veralteten Daten von diesem Speicherort.
2. Löschen Sie alle darin enthaltenen Dateien und Ordner:

C:/ProgramData/Cisco/Cisco Secure Client/Umbrella/

Vorsicht: Möglich. Die hier genannten Details enthalten Verfahren oder Befehle, die bei Ausführung erhebliche Auswirkungen haben können. Stellen Sie sicher, dass die oben genannten Verfahren oder Befehle von einem SME oder einer Geschäftseinheit evaluiert wurden, bevor Sie sie ausführen oder empfehlen.

Laden Sie die Datei New OrgInfo.json hoch.

1. Legen Sie die neu heruntergeladene OrgInfo.json in den dafür vorgesehenen Umbrella-Ordner.
2. Kopieren Sie die neue Datei OrgInfo.json in:

C:/ProgramData/Cisco/Cisco Secure Client/Umbrella/

Starten Sie den Cisco Secure Client Service neu.

Initialisieren Sie den Cisco Secure Client erneut, damit die Änderungen wirksam werden. Starten Sie den Dienst Cisco Secure Client - AnyConnect VPN Agent von Windows Services.

(Wenn Problem weiterhin besteht) Erfassen Sie Diagnosedaten für weitere Analysen.

Wenn das Gerät immer noch nicht registriert werden kann, erstellen Sie ein neues DART-Paket,

um eine tiefere Fehlerbehebung zu ermöglichen. Verwenden Sie das DART-Tool in Cisco Secure Client, um ein neues Diagnosepaket zu sammeln.

Nach der Durchführung dieser Schritte muss das Umbrella-Modul von einem "Deaktiviert"-Status in einen Betriebsstatus übergehen und die DNS-Sicherheitsfunktionen wie vorgesehen aktivieren.

Ursache

Die Ursache des Problems war eine ungültige oder veraltete Datei "OrgInfo.json" mit einem falschen Fingerabdruckwert. Diese Abweichung führte zu fehlerhaften Geräteregistrierungsanforderungen an die Umbrella-API, was dazu führte, dass das Modul deaktiviert blieb. Der Fehler wurde durch Protokolleinträge bestätigt, die während der Registrierungsversuche "Fingerabdruck stimmt nicht überein" und "Gerät-ID konnte nicht erstellt werden" zeigten.

Beispielprotokoll-Auszug aus DART-Protokollen:

```
{"error":"invalid_request","message":"fingerprint does not match","code":400,"code_text":"Bad Request"}  
Device Registration: failed to create device id
```

Verwandte Inhalte

- [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.