Beheben von Verbindungsproblemen mit Cowork (Frontier)-Agenten, wenn Umbrella aktiviert ist

Inhalt

Problem

Der Cowork (Frontier) Agent funktionierte nicht ordnungsgemäß auf Laptops, als Cisco Umbrella aktiviert wurde. Als Cisco Umbrella inaktiv war, funktionierte der Agent wie erwartet. Die Benutzer konnten die Cowork-Agent-Funktion nicht verwenden, als Umbrella aktiv war, und in Cisco Umbrella waren keine Blockprotokolle sichtbar, als das Problem bei den Benutzern auftrat. Es wurden Fehler-Screenshots bereitgestellt, die die Anwendungsfehler während des Umbrella-Vorgangs zeigen.

Umwelt

- Cisco Umbrella auf Enterprise-Laptops bereitgestellt
- Cowork (Frontier) Agent Applikation
- SSL/TLS-Datenverkehrsanalyse in Cisco Umbrella aktiviert
- In der Cowork-Anwendung implementierte Zertifikatpinning

Auflösung

Das Problem wurde durch Hinzufügen der Cowork-Anwendung zur Liste "Do Not Decrypt (DND)" in Cisco Umbrella behoben. Durch diese Konfigurationsänderung kann der Cowork Agent die SSL/TLS-Prüfung umgehen und seine direkte verschlüsselte Verbindung zu den Cowork-Servern aufrechterhalten.

Schritte zum Konfigurieren der DND-Liste

Schritt 1: Rufen Sie das Cisco Umbrella Dashboard auf, und navigieren Sie zur Konfiguration der SSL-Entschlüsselungsrichtlinie.

Phase 2: Fügen Sie Cowork-bezogene Domänen und URLs zur Liste Nicht entschlüsseln hinzu, um die SSL-Überprüfung für diese Anwendung zu umgehen.

Schritt 3: Wenden Sie die Richtlinienänderungen an, und warten Sie, bis die Konfiguration auf alle Endpunkte verteilt wird.

Schritt 4: Testen Sie die Funktionalität des Cowork Agent mit aktiviertem Cisco Umbrella, um den ordnungsgemäßen Betrieb zu überprüfen.

Validierung

Nach der Implementierung der Konfiguration der DND-Liste funktionierte die Cowork-Anwendung normal, wobei Cisco Umbrella aktiviert war. Interne Tests bestätigten, dass das Problem mehrere Tage nach der Überwachung nicht erneut auftrat und alle Benutzer erwartungsgemäß auf die Cowork-Funktionalität zugreifen konnten.

Ursache

Der Cowork (Frontier)-Agent verwendet die Zertifikatsanheftung als Sicherheitsmechanismus. Zertifikatfixierung bedeutet, dass die Anwendung so programmiert ist, dass sie nur ihr eigenes Serverzertifikat akzeptiert und diesem vertraut. Wenn Cisco Umbrella den Datenverkehr abfängt und das Cisco Zertifikat anstelle des ursprünglichen Serverzertifikats präsentiert, erkennt die Cowork-Anwendung diese Änderung, geht davon aus, dass die Verbindung nicht sicher ist, und verwirft absichtlich die Verbindung, um die Daten zu schützen. Dies ist ein erwartetes Verhalten für Anwendungen, die Sicherheitsmaßnahmen für die Zertifikatspinning implementieren.

Verwandte Inhalte

- Erstellen einer effektiven Liste nicht entschlüsseln für Microsoft-Anwendungen
- 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.