Umbrellaを有効にした場合のCowork(Frontier)エージェント接続の問題の解決

内容

問題

Cisco Umbrellaを有効にしたときに、Cowork(Frontier)エージェントがラップトップで正しく動作しませんでした。Cisco Umbrellaが非アクティブになると、エージェントは期待どおりに機能しました。Cisco Umbrellaがアクティブなときにユーザがエージェント機能を使用できず、この問題が発生したときにCisco Umbrellaでブロックログが表示されませんでした。Umbrella操作中のアプリケーションエラーを示すエラースクリーンショットが提供されました。

環境

- 企業のラップトップに導入されたCisco Umbrella
- Cowork(Frontier)エージェントアプリケーション
- Cisco UmbrellaでのSSL/TLSトラフィックインスペクションの有効化
- Coworkアプリケーションに実装された証明書ピニング

解決方法

この問題は、Cisco UmbrellaのDo Not Decrypt(DND)リストにCoworkアプリケーションを追加することで解決しました。この設定変更により、Coworkエージェントは SSL/TLSインスペクションをバイパスし、Coworkサーバへの直接暗号化された接続を維持できます。

DNDリストの設定手順

ステップ1:Cisco Umbrellaダッシュボードにアクセスし、SSL復号化ポリシー設定に移動します。

ステップ2：このアプリケーションのSSLインスペクションをバイパスするために、仕事関連のドメインとURLをDo Not Decryptリストに追加します。

ステップ3:ポリシーの変更を適用し、設定がすべてのエンドポイントに伝播されるまで待機します。

ステップ4:Cisco Umbrellaを有効にしてCowork agentの機能をテストし、正常に動作していることを確認します。

検証

DNDリストの設定を実装した後、Cisco Umbrellaを有効にするとCoworkアプリケーションが正常に機能しました。社内テストでは、数日の監視期間中に問題が再発しなかったことが確認され、すべてのユーザがCowork機能に期待どおりにアクセスできることが確認されました。

原因

Cowork (Frontier)エージェントは、証明書ピニングをセキュリティメカニズムとして使用します。証明書のピニングとは、アプリケーションが特定のサーバ証明書だけを受け入れて信頼するようにハードコードされていることを意味します。Cisco Umbrellaがトラフィックを代行受信し、元のサーバ証明書の代わりにCisco証明書を提示すると、Coworkアプリケーションはこの変更を検出し、接続がセキュアではないと想定し、データを保護するために意図的に接続をドロップします。これは、証明書ピニングのセキュリティ対策を実装するアプリケーションで想定される動作です。

関連コンテンツ

- Microsoftアプリケーション用の有効な非暗号化機能リストの作成
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。