セキュアアクセスでのWhatsAppに関するDLPポリシーの制限

内容

お問い合わせ内容

HTTPS復号化が有効になっているにもかかわらず、WhatsApp（ブラウザまたはデスクトップアプリケーション）を介して共有される場合、Cisco Secure Access(CSA)のDLPポリシーによって機密ファイルが検出されたり、ブロックされたりすることはありません。DLPエンジンはこれらのプラットフォームを介したファイルアップロードのトリガーまたは検出に失敗しますが、同じDLPポリシーが他のオンラインアップロードツールを介してアップロードされた同じファイルを正常にブロックします。WhatsAppの基本的なアップロードブロッキングをテストすると、この機能はブラウザとデスクトップの両方のバージョンで正しく動作しますが、問題はDLPポリシーの適用に特に分離されています。

環境

- シスコセキュアアクセス
- 設定済みのDLPポリシー
- HTTPS暗号化解除が有効
- WhatsApp WebおよびWhatsAppデスクトップアプリケーション

解決策

観察された動作は、エンドツーエンド暗号化(E2EE)の実装と非標準トラフィック処理によるWhatsAppおよび類似のプラットフォームの予想制限です。次のセクションで概説するトラブルシューティング手順と回避策を実装できます。

検証ステップのトラブルシューティング

回避策を実装する前に、次の項目を確認してください。

- 正しいSWG IDおよび送信元IDが設定されていることを確認します。
- HTTPSインスペクション/復号化が有効であり、ターゲットプラットフォームに対して選択的にバイパスされていないことを確認します。
- Isolation/RBIおよびAllow-Override設定が正しく設定されていることを確認します。
- DLPポリシーがグループベースの場合、ADグループメンバーシップを確認します。
- 除外されているトラフィックのTraffic Steering Bypassリストを確認します。
- ブラウザでQUICプロトコルが無効になっていることを確認します。
- インスペクションをバイパスする可能性のあるIPv6トラフィックの影響を確認します。

推奨される回避策

WhatsApp Webトラフィックに対してDLP強制を有効にするには、WhatsApp Web宛てのトラフィックに対してリモートブラウザ分離(RBI)を実装します。この回避策により、ブラウザセッションを分離し、分離された環境内でコンテンツインスペクションを有効にすることで、DLPポリシーを適用できます。

WhatsApp Webドメイン専用にRBI強制を設定し、Webインターフェイスを介したファイルアップロードとコンテンツ共有がDLPポリシー評価の対象となるようにします。

追加情報

この制限に関して、製品の機能拡張の要求が文書化されています(CSE-I-1249)。

原因

WhatsApp（WhatsApp Webを含む）および同様のコラボレーションプラットフォームは、エンドツーエンド暗号化(E2EE)を実装し、メッセージテキストとファイルのアップロードに対するフルコンテンツインスペクションとスキャニングを防止します。また、WhatsAppトラフィックは通常のWebアップロードと同じ方法で標準のHTTP/HTTPSポートを使用しないため、Secure Web Gateway(SWG)は通常のHTTPS検査パスを介してトラフィックを代行受信して検査することができません。この暗号化およびトラフィック処理方法は設計上の制約があり、これらの特定のプラットフォームに対する現在のDLP検査機能の予想される制限を表します。

関連コンテンツ

- 製品の機能拡張の要求CSE-I-1249
- 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。