シスコセキュアアクセスのフラグメント化ICMPパケット処理

内容

お問い合わせ内容

MTUよりも大きいICMPエコー要求は、DF(Don't Fragment)ビットを無効にして送信された場合に応答を受信しません。この動作は、次の2つの特定のシナリオで発生します。

- DFビットがクリアされた状態で、VPNインターフェイスのMTUサイズを超えるICMPパケットをVPNインターフェイス経由で送信する場合
- DFビットがクリアされた状態で、IPsecトンネルインターフェイスのMTUサイズを超えるICMPパケットを送信する場合に、サイトルータとCisco Secure Access(CSA)間のIPsecトンネルを経由してオンプレミスのエンドポイントから送信する

いずれの場合も、ICMP応答が受信されないため、DFビットが無効になっているフラグメント化されたパケットがCSAでドロップされるかどうかについて疑問が生じます。

環境

- シスコセキュアアクセス(CSA)
- RAVPN (リモートアクセスVPN) エンドポイント
- サイトルータとCSA間のIPSecトンネル
- インターフェイスMTUサイズを超過したICMPトラフィック
- DFビットがクリアされたフラグメント化パケットシナリオ

解決策

シスコセキュアアクセスは、アンダーレイとオーバーレイの両方のシナリオでフラグメント化されたパケットをドロップします。この動作は、Cisco Secure Accessのヘルプドキュメントに「ア

ンダーレイまたはオーバーレイ内のフラグメント化されたパケットはドロップされる」と明示的に記載されています。

予想される動作

シスコセキュアアクセスは、アンダーレイネットワークまたはオーバーレイネットワークのどちらでフラグメント化パケットが発生しているかにかかわらず、それらのパケットを廃棄するように設計されています。これは次の製品に適用されます。

- DFビットがクリアされた状態で、VPNインターフェイスMTUを超えるRAVPNエンドポイントから送信されたICMPパケット
- DFビットがクリアされた状態で、トンネルインターフェイスMTUを超えるIPsecトンネル経由でオンプレミスのエンドポイントから送信されたICMPパケット

この動作は、Cisco Secure Accessインフラストラクチャ内のフラグメント化されたパケットに関係するすべてのシナリオで一貫しています。

これに対して機能要求CSE-I-5739が作成されています。

原因

シスコセキュアアクセスは、セキュリティおよびパフォーマンス設計の決定として、フラグメント化されたパケットをドロップするように設計されています。この動作は、アンダーレイとオーバーレイネットワークの両方のシナリオで、潜在的なセキュリティの脆弱性と、パケットの再構成に関連する処理のオーバーヘッドを防ぐために実装されます。

関連コンテンツ

- Cisco Secure Accessヘルプドキュメント – 断片化パケットの処理
- 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。