MacOS上のBroadcom WSSとのUmbrella DNSセキュリティ共存の問題

内容

お問い合わせ内容

Broadcom WSS(Web Security Service)と共存している場合、UmbrellaモジュールはmacOS上のDNSトラフィックを代行受信しません。 80や443などの特定のWebポートを代行受信するようにWSSエージェントが設定されている場合、Umbrella DNSセキュリティ機能はすべてのDNSクエリのキャプチャに失敗します。ただし、WSSが無効になっている場合、UmbrellaはDNSトラフィックの傍受を期待どおりに再開します。WSSが有効な場合、すべてのDNSトラフィックが代行受信されるのではなく、特定のDNSクエリのみがUmbrellaによって処理されます。

環境

- オペレーティングシステム：macOS
- Cisco Umbrella DNSセキュリティモジュール
- Broadcom WSS（Webセキュリティサービス）エージェント
- Webポート80および443を代行受信するように設定されたWSSエージェント

解決策

この問題は分析の結果、現在のmacOSアーキテクチャではDNSセキュリティがWSSと共存できない、macOSのアーキテクチャ上の制限であると判断されました。この制限は、InfobloxとCisco Umbrellaの両方のDNSセキュリティソリューションに適用されます。

技術分析

根本原因は、macOSのDNSプロキシの制限に関連しています。

- macOSの制限により、システムで同時にアクティブにできるDNSプロキシは1つだけです
- DNSリゾルバがutunXインターフェイスまたはプロキシ挿入リゾルバにバインドされている場合、macOSはUmbrellaではなくトンネル内でDNSを解決します
- macOSで別のNEDnsProxyProviderがシステム上でアクティブになっている場合、UmbrellaはDNSトラフィックを代行受信しません

診断コマンド

macOSで優先されるDNSリゾルバを確認するには、次のコマンドを使用します。

```
scutil --dns
```

このコマンドは、スコープ指定、補足、またはインターフェイス： utunXとしてマークされているリゾルバを表示し、DNSプロキシの競合を特定するのに役立ちます。

回避策のオプション

macOS環境では、WSSは個別のDNSエージェントなしでDNSの代行受信を続行します。DNSセキュリティカバレッジを進めるには、パッシブバイパスアーキテクチャをサポートするように実装するという選択肢があります。このアプローチでは、プロバイダーはフローを完全にバイパスし、プロバイダーがアクティブでなかったかのようにトラフィックを処理できます。

原因

この問題は、システム上で同時に1つのNEDnsProxyProviderしかアクティブにできないというmacOSアーキテクチャの制限が原因で発生します。Umbrella DNSセキュリティとBroadcom WSSの両方をインストールすると、両方がDNSプロキシ制御を競合するため、WSSが優先され、UmbrellaがDNSトラフィックを傍受しなくなります。これは、macOSネットワーキングスタックの基本的な制限であり、Cisco Umbrellaだけでなく、すべてのDNSセキュリティソリューションに影響します。

関連コンテンツ

- 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。