

リンクローカルAAAサーバアドレスによるセキュアアクセスRA VPN認証イベント

内容

問題

セキュアアクセスリモートアクセス(RA)VPN機能をテストすると、テナント組織に存在しないIDに対して過剰な認証イベントがログに記録されます。認証ログには、24時間以内に「AAALOG_SERVICE_DOWN」や「AAALOG_SERVER_DOWN」などのAAAエラーを含む、10,000を超えるRA VPN認証イベントが表示されます。これらのエラーメッセージは、テナントで設定されていないAAAサーバとしてリンクローカルアドレス169.254.x.xを参照します。

ログに記録される特定のエラー例は次のとおりです。

```
AAALOG_SERVICE_DOWN
AAA authentication server not accessible : server = 169.254.169.79 : user = <user>
```

```
AAALOG_SERVER_DOWN
AAA Marking RADIUS server 169.254.169.79 as FAILED
```

このアクティビティは、Secure Access VPN FQDNに対してRADIUSベースの認証を繰り返し試行することで、過剰なログノイズを生成し、外部スキャンやVPNサービスの潜在的な悪用に関する懸念を生み出しています。

環境

- Cisco Secure Accessプラットフォーム
- リモートアクセスVPNプロファイルが証明書認証なしで初期設定されている
- RA VPNに設定されたRADIUSベースの認証
- 検出可能なVPNプロファイルを使用したパブリックVPNテナント設定

解決方法

この問題を解決するには、認証フローの動作を理解し、緩和戦略として証明書ベースの認証を実装する必要がありました。

確認された動作に関する技術的説明

過剰な認証イベントは、次のセクションで説明する技術上の理由により発生します。

証明書要件のない認証フロー

証明書認証が無効で、RADIUSベースのRA VPN認証が使用されている場合、システムでは、最初にセキュアアクセスで同期されたユーザのデータベースと照合してユーザ名IDをチェックし、「認証の失敗」イベントを記録するため、「認証の失敗」試行がログに記録されます。これらのイベントは最初の防衛線として期待されますが、外部の攻撃者が認証を試みると大きなログノイズが発生する可能性があります。

リンクローカルアドレスの使用

ログに表示される169.254.x.xのアドレスは、RA VPNヘッドエンドが着信セッションを許可するために使用する内部/ローカルリンクアドレスです。これらのアドレスは、テナント内のAAAサーバの設定ミスではなく、内部システムの動作を表しています。

VPNプロファイルの検出

パブリックVPNテナントIDが設定されると、UIドロップダウンにVPNプロファイルが表示されます。これにより、外部のアクターはパブリックプロファイルをより簡単に検出し、認証試行の対象にすることができます。

即時の対応策

1. – 証明書ベースの認証を設定します。証明書ベースの認証を要求するようにRA VPNプロファイルを変更します。証明書認証が必要な場合、セキュアアクセスは認証フローの前半で証明書チェックを実行します。証明書が見つからない場合、システムは標準の認証フローの前にエラーを生成し、「認証の失敗」イベントは同じ方法でログに記録されません。

2. – 軽減の効果を検証します。証明書ベースの認証を実装した後の認証ログを監視し、過剰な認証イベントの減少を確認します。証明書ベースの認証に切り替えることで、攻撃が軽減され、ログノイズが減少しました。

長期的な改善

根本的な問題に対処するために、次の2つの機能要求が作成されました。

- 機能要求1：パブリックVPNテナントの追加時にトンネルグループ（VPNプロファイル）リストの表示/非表示を切り替えるオプションを追加し、プロファイルの検出可能性を低下させます。
- 機能要求2：失敗したRA VPN認証試行のロギングを有効または無効にする設定オプションを追加し、管理者がログの冗長性を制御できるようにします。

また、ログに記録されたイベントと認証の動作を説明して、管理者が通常システム動作を理解しやすくするために、公開ドキュメントが作成されます。

原因

過剰な認証イベントの根本原因は、パブリックテナント設定の検出可能なVPNプロファイルと、証明書ベースの認証が不要な場合の認証フローの動作の組み合わせです。証明書要件なしでRADIUSベースの認証が使用される場合、システムでは、VPNプロファイルを検出する外部のアクターからの試行を含め、セキュリティポスチャの一部としてすべての「認証の失敗」試行がログに記録されます。ログ内のリンクローカルアドレスは、RA VPNヘッドエンド認証プロセスの通常の内部システム動作を表しており、設定エラーを表していません。

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。