ゼロトラストアクセスプロファイルの削除によるユーザアクセスの損失

内容

お問い合わせ内容

未使用であると考えられていたゼロトラストアクセス(ZTA)プロファイルを削除した後、ZTNAモジュールを使用するすべてのユーザで、プライベートリソースとインターネットナビゲーションの両方へのアクセスが完全に失われました。このプロファイルを削除すると、すべてのZTNAユーザのサービスが即座に中断され、Zero Trust Network Accessインフラストラクチャを介してリソースにアクセスできなくなります。

影響を受けたユーザは、以下への接続を確立できませんでした。

- プライベート内部リソース
- ZTNAモジュール経由のインターネットナビゲーション

環境

- セキュアなアクセス (ゼロトラストネットワークアクセス)
- 複数のユーザプロファイルを使用して導入されたZTNAモジュール
- ZTNA制御で設定されたデフォルトポリシー
- ユーザアクセス管理用に設定された複数のZTAプロファイル

解決策

ZTAプロファイルの照合ロジックについて

ゼロ信頼アクセスプロファイルは、特定の照合順序とロジックに基づいて適用されます。

- プロファイルの照合順序：ZTAプロファイルは、ユーザと宛先の照合基準に基づく順序で評価されます
- デフォルトプロファイルの動作：ユーザまたは宛先の基準に一致する特定のプロファイルがない場合は、デフォルトプロファイルにフォールバックします
- プロファイルの依存関係：有効なデフォルトとして機能するプロファイルを削除すると、未使用のように見えてもサービスが中断される可能性があります

削除されたプロファイルは、設定インターフェイスでは使用されていないように見えますが、ユーザ照合の有効なデフォルトプロファイルとして機能している可能性があります。このプロファイルが削除されると、ユーザはZTNAインフラストラクチャを介したプライマリアクセスパスを失います。

検証手順

今後も同様の問題が発生しないように、次の検証アプローチを実装する必要があります。

1. – 削除する前に、設定されているすべてのZTAプロファイルとその照合基準を確認します。

2. – ユーザアクセスの有効なデフォルトとして機能するプロファイルを特定します。

3. – 設定のスクリーンショットとポリシーの確認を通じて、ユーザとプロファイルのマッピングを確認します。

4. – 生産に適用する前に、管理された方法でプロファイルの変更をテストします。

原因

根本的な原因は、ZTNAユーザアクセスの有効なデフォルトプロファイルとして機能していたZTAプロファイルが、設定インターフェイスでは使用されていないように見えても削除されたこ

とです。このプロファイルが削除されると、システムはユーザアクセスのプライマリー致基準を失い、すべてのZTNAユーザはプライベートリソースとインターネットナビゲーションの両方への接続を失うことになります。プロファイル照合ロジックは、特定のユーザまたは宛先の基準が他の設定済みプロファイルによって満たされていない場合に、フォールバックに使用できる有効なデフォルトプロファイルがあるかどうかによって異なります。

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。