VPNプロファイル名の長さの制限によるセキュアアクセスVPN管理者のリセット切断

内容

お問い合わせ内容

リモートアクセスVPNユーザで、アクティブセッション中にCisco Secure Accessで断続的な切断が発生しました。Cisco Secure Access(CSA)のログには、この時点でスケジュールされたメンテナンス作業が発生していないにもかかわらず、Administrator Resetとしてこれらの切断イベントが記録されています。この切断は、通常の業務運用中にリモートアクセスユーザに影響を与え、ユーザがVPNサービスにアクティブに接続している間に予期しないセッションの終了を引き起こしました。

接続解除イベントは、管理者リセットエントリとしてリモートアクセスログに記録されます。管理者リセットエントリは、通常、管理介入またはシステムが開始したセッションの終了を示します。ただし、報告されたタイムフレーム中にシステムに対して管理操作は実行されませんでした。

環境

- Cisco Secure Access(CSA)：リモートアクセスVPNサービス
- 名前の長さが46文字を超えるVPNプロファイル設定

解決策

この問題の解決には、管理者リセットイベントを引き起こすVPNプロファイル名の長さの制限に対処するための回避策の実装が含まれます。

当面の回避策

ステップ1：名前が46文字を超えるVPNプロファイルを特定する

Cisco Secure Accessダッシュボードで既存のすべてのVPNプロファイル設定を確認し、46文字を超える名前のプロファイルを特定します。

ステップ2:VPNプロファイルの名前を文字数制限に合わせて変更する

46文字を超えるすべてのVPNプロファイルの名前を、46文字以下に変更します。これは、Cisco Secure Access管理インターフェイスを介して実行できます。

ステップ3：切断イベントの監視

VPNプロファイル名の変更を実装した後、リモートアクセスログを監視して、管理者リセットイベントが通常の運用中に発生しなくなったことを確認します。

長期的なソリューション

VPNプロファイル名がバックエンド処理の制限を超える可能性のあるGUIの制限に対処するために、永続的な修正が開発されています。この修正により、ユーザインターフェイスレベルで46文字の制限が適用され、バックエンド処理の問題を引き起こす名前を持つVPNプロファイルの作成が防止されます。

開発チームは、作成および変更時にVPNプロファイル名の長さを制限する適切な検証をGUIに実装することに取り組んでいます。これにより、この問題が将来の設定で発生することを防ぎます。

その他の考慮事項

場合によっては、クライアントデバイスのWi-Fiアダプター電源管理設定が接続問題の原因となることがあります。VPNプロファイル名の長さ修正を実装した後も接続の切断が続く場合は、該当するクライアントデバイスでWi-Fiアダプタの省電力機能が無効になっていることを確認してくだ

さい。無効になっている設定では、再接続イベントがログにAdministrator Resetエントリとして表示される可能性があります。

原因

管理者リセットイベントの根本原因は、Cisco Secure Accessのバックエンド処理の制限です。この制限では、46文字を超えるVPNプロファイル名がセッション管理中にシステムエラーを引き起こします。バックエンドシステムでこの制限を超える名前のVPNプロファイルが検出されると、保護措置として管理者リセットがトリガーされ、影響を受けるセッションが終了します。

この問題は、GUIインターフェイスではユーザが46文字を超えるVPNプロファイル名を作成できますが、バックエンド処理システムでは46文字に制限されているために発生します。バックエンドで長いストリングが処理されると、Administrator Resetイベントがログに記録され、関連するVPNセッションの切断が強制されます。

関連コンテンツ

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。