

Googleドライブセキュアダウンロード中の CRYPTO_INTERNAL_ERROR

内容

お問い合わせ内容

暗号化されたGoogleシートファイルは、トラフィックの復号化が有効なCisco Secure Accessを介してアクセスすると開くことができません。Googleドライブのセキュアダウンロード中にCRYPTO_INTERNAL_ERRORが発生しました。この問題は、特にセキュアWebゲートウェイ(SWG)インスペクションがアクティブな場合に発生します。復号化およびインスペクションプロセス中に範囲ヘッダーが無視され、Googleのセキュアダウンロードメカニズムに干渉が発生するためです。

この問題は、RAVPN+ZTAの実装を使用している環境に影響を与え、多数のユーザが暗号化されたGoogleシートにアクセスする際に影響を与えます。

環境

- テクノロジー：Cisco Secure Access (ソリューションサポート)
- サブテクノロジー：セキュアなアクセス
- 実装：RAVPN+ZTA (リモートアクセスVPN +ゼロトラストアクセス)
- 該当コンポーネント：ZTAプロファイル
- 影響を受けるドメイン：clients6.google.comおよびその他のGoogleドライブ関連ドメイン

解決策

この問題を解決するには、永続的なベンダー側の修正を監視しながら、一時的な回避策を実装す

る必要があります。

次のセクションで概説するアプローチは、暗号化されたGoogleシートへのアクセスを復元するために検証されています。

一時的な回避策のオプション

オプション1：トラフィックの復号化を無効にする

影響を受けるユーザグループまたはポリシーのトラフィック復号化を完全に無効にします。これにより、Google Sheetsのアクセスは復元されますが、復号化ベースのセキュリティ検査機能はすべて削除されます。

オプション2：復号からGoogleドライブドメインを除外する

Googleドライブ関連のドメインを、セキュアアクセスポリシー設定のdo-not-decryptリストに追加します。

- clients6.google.com
- トラフィック分析で特定されたその他のGoogleドライブ関連ドメイン

このアプローチでは、他のトラフィックの復号化を維持しながら、Googleシートを正常に機能させることができます。ただし、この回避策には、除外ドメインのCASB Googleドライブのアップロードブロック機能を無効にするトレードオフがあります。

技術分析とモニタリング

シスコの分析により、Secure Web Gatewayインスペクションでは、ファイルコンテンツの包括的なセキュリティスキャンを可能にするために範囲ヘッダーが無視されることが確認されました。この動作は、Googleドライブの安全なダウンロードプロセスを妨げます。このプロセスは、適切な復号化フローの範囲ヘッダーに依存します。

Googleはこの問題を認識し、プロキシの動作 (Cisco Umbrella/ネットワークプロキシを含む) が Rangeヘッダーを削除または書き換えることにより、Googleドライブの安全なダウンロード要求を妨げていることを特定しました。これにより、Googleの復号化メカニズムを破るフルファイルのダウンロードが強制されます。Googleはクライアント側の修正を開発中ですが、到着予定時刻は提供されていません。

実装に関する考慮事項

回避策を実装する組織は、セキュリティへの影響を考慮する必要があります。

- 復号検査からGoogleドライブドメインを除外するリスクを評価します。
- ドメイン除外の影響を受ける可能性のあるCASBポリシーを確認します。
- 将来のポリシーのレビューに備えて、回避策の一時的な性質を文書化します。
- クライアント側の修正プログラムの開発に関するGoogleからの更新を監視します。

原因

根本原因は、Cisco Secure Access SWGインスペクションの動作とGoogleドライブのセキュアダウンロードメカニズムの間の互換性の問題です。

具体的には、

Cisco Secure Web Gatewayインスペクションは、復号化およびセキュリティスキャンプロセス中に範囲ヘッダーを無視して、完全なファイル分析を保証します。ただし、Googleドライブで暗号化されたファイルアクセスは、範囲ヘッダーを使用して、セキュアなダウンロードの復号化フローを適切に処理します。プロキシ検査プロセス中にこれらのヘッダーが削除または変更されると、Googleクライアント側での復号化が失敗し、CRYPTO_INTERNAL_ERRORが発生します。

これは、セキュリティ検査要件 (完全なファイルスキャン) とGoogle暗号化ファイル配信メカニズム (範囲ベースの安全なダウンロード) の間の基本的な非互換性を表します。

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。