Splunkクライアントログのアップロードによるセキュアアクセス証明書の検証エラー

内容

お問い合わせ内容

Splunkクライアントを実行しているWindowsクライアントは、トラフィックがCisco Secure Accessによって復号化されたときに証明書検証エラーが発生したため、Splunkクラウドにログをアップロードできませんでした。5,000を超えるWindowsのログソースがSplunkクラウドへのデータ送信に失敗し、ログの取り込みに影響を与えました。Splunkクライアントのログに記録されたエラーは次のとおりです。

```
02-27-2026 16:51:54.830 +0530 ERROR X509Verify [15668 TcpOutEloop] - Server X509 certificate failed val
```

宛先*.splunkcloud.comへのトラフィックはファイアウォール経由で流れていましたが、アプリケーションレベルの証明書の検証は失敗しました。SSL復号化が有効になっているサイトへのWebブラウズは正常に動作し続けました。

環境

- SSL/TLS復号化が有効なCisco Secure Access
- Splunk Universal Forwarderがインストールされ

解決策

この問題は、Cisco Secure AccessでSplunkクラウドトラフィックの復号化バイパスポリシーを実装することで解決されました。

いくつかの措置が講じられた。

ステップ1：問題の特定

WebExセッション中に、動作が確認され、再現されました。テストでは、クライアントでセキュアアクセスの復号化が無効にされたとき、またはクライアントでSWGサービスが無効にされたとき、Splunkログのアップロードが成功したことが示されました。これにより、SSL/TLS復号化プロセスが証明書検証の失敗の原因となっていることが確認されました。

ステップ2：通知先リストの作成

SplunkクラウドのFQDNとIPアドレスを含む宛先リストが作成され、Splunkクラウドサービス宛てのトラフィックを対象に指定されました。

ステップ3：復号バイパスポリシーの実装

Splunkクラウドの宛先リストと一致するトラフィックのSSL/TLS復号化を無効にするために、Cisco Secure Accessポリシーが実装されました。このバイパスポリシーにより、Splunkクライアントは、セキュアアクセスによる証明書の傍受を行わずに、Splunkクラウドへの暗号化された直接接続を確立できました。

ステップ4：検証

復号化バイパスポリシーを実装した後、検証によって次のことが確認されました。

- Splunkクライアントがログを正常にアップロードできました
- Splunkクラウドのレポーティングクライアントの総数は大幅に増加しました
- 証明書の検証エラーは確認されませんでした

ケースの重大度は1から3に下げられ、ログの継続的な取り込みの成功を監視するモニタリングステータスに設定されました。

原因

根本的な原因は、Splunkクライアントが独自の証明書ストアを使用しており、SSL/TLS復号化中に提示されたCisco Secure Accessプライマリ SubCA証明書を信頼していないことにあります。シスコセキュアアクセスがSplunkクラウドへのSSLトラフィックを代行受信して復号化すると、独自の認証局を使用してトラフィックが再暗号化されます。Splunkのクライアント証明書検証プロセスは、自身の証明書ストア内の信頼されたルート認証局に戻る証明書チェーンを検証できなかったため、この証明書を拒否しました。

特定のX.509検証エラー「unable to get local issuer certificate」（エラーコード20）は、証明書検証プロセスで、クライアントの信頼できる証明書ストアに発行側の認証局を見つけることができず、接続が失敗したことを示します。

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。