お客様各位

シスコのエンジニアリング部門では、ご使用のリリースについて、このソフトウェアの使用に影響を及ぼす可能性がある以下のソフトウェアの問題を確認しました。このソフトウェアアドバイザリ通知を参照して、お客様の環境に該当する問題かどうかを確認してください。説明されている問題が該当しなければ、このソフトウェアのダウンロードに進むことができます。

このソフトウェアに含まれる内容の詳細については、製品セレクタツールから入手可能なシスコソフトウェアのリリースノートを参照してください。このページから、関心のある製品を選択します。リリースノートは、製品ページの「一般情報」にあります。

アドバイザリの理由：
このソフトウェアアドバイザリでは 1 つのソフトウェアの問題に対処します。

CSCvh22181
SSL インスペクションが有効になっている TLS 1.3 を使用した Web サイトのロードが失敗する

影響を受けるプラットフォーム：
すべての物理および仮想の管理対象デバイス（つまり、Firepower Threat Defense および Cisco ASA with FirePOWER Services を実行するデバイス）

症状：
SSL インスペクションポリシーが有効になっている場合、SSL 復号ルールに一致するトラフィックの TLS 1.3 接続が失敗します。

2018 年 3 月以降、特定の Web ブラウザは、TLS 1.2 トラフィックよりも TLS 1.3 トラフィックを優先するように更新されています。その場合、TLS 1.3 をサポートするブラウザと Web サイトの間の接続は確立できません。

ユーザーのブラウザには、次のエラーが表示されます。

```
ERR_SSL_VERSION_INTERFERENCE
```

また、TLS バージョン 1.3 トラフィックは復号も検査もされません。

状況：
- 管理対象デバイスで SSL インスペクションポリシーが有効になっている
- ブラウザの更新により、 TLS 1.3 がブラウザで有効になっている

- TLS 1.3 をサポートしている Web サイトをユーザーが参照する

回避策：
各管理対象デバイスを設定して、TLS 1.3 のサポートを削除し、代わりに暗号化された接続が TLS 1.2 を使用してネゴシエートされるようにします。

管理対象デバイスで、次の手順を実行します。

- SSH クライアントを使用して CLI にログインし、管理 IP アドレスに接続します。`admin` ユーザー名（デフォルトのパスワードは `Admin123` です）または別の CLI のユーザーアカウントを使用してログインします。

  詳細については、次を参照してください。
- Firepower Threat Defense デバイス：Firepower Threat Defense デバイス用の『Command Reference for Firepower Threat Defense』にある CLI の使用に関する章
- 従来型デバイス：『Firepower Management Center Configuration Guide』の「Logging Into the Command Line Interface on Classic Devices」
- > プロンプトで、次のコマンドを入力します。

  ```
  system support ssl-client-hello-tuning extensions_remove 43
  ```

  （「43」は TLS 1.3 プロトコルの識別子です）
- 画面に表示される指示に従って、検出エンジンである Snort を再起動します。次に例を示します。

  ```
  pmtool restartbytype DetectionEngine
  ```

- 次のコマンドを入力して、設定の変更を確認します。

  ```
  system support ssl-client-hello-display
  ```

正常に変更されたことを確認するために、次のメッセージが表示されます。
`extensions_remove=43`

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。