# 目次



# 概要

この資料は許可されていないユーザが保護されたコンテンツにアクセスすることを可能にする Cisco 適応性があるセキュリティ アプライアンス モデル（ASA） sowftware 内の脆弱性を記述したものです。 この問題のための回避策はまた記述されています。

# 問題

攻撃者によって SSL/TLS （獣）脆弱性に対するブラウザ エクスプロイトが効果的に Cipher Block Chaining （CBC）暗号化モードの初期化ベクトル（iv）チェーニング

攻撃はツールを使用します広く利用された Transport Layer Security バージョン 1 （TLSv1）プロトコルの脆弱性を不正利用する。 問題プロトコル自体はで、むしろ使用する暗号スイート定着しませんが。 TLSv1 および Secure Sockets Layer バージョン 3 （SSLv3）は埋め込み Oracle 攻撃が発生する CBC 暗号を支持します。

# ユーザインパクト

SSL サーバの 75% 上の信頼できるインターネット移動が、 SSL パルス SSL 実装アンケート

# 解決策

獣はプロトコルによって使用する暗号の脆弱性のエクスプロイトです。 それが CBC 暗号に影響を与えるので、この問題のためのオリジナル回避策は RC4 暗号へ代りに切り替えることでした。 ただし、 RC4 技術情報のキー スケジューリングアルゴリズムの弱さは RC4 に不適当にさせた脆弱性があったことを明らかにします。

回避策はこの問題、Cisco ASA のためのこれら二つの修正を設定しました:

- Cisco バグ ID CSCts83720: *TLS 1.1/1.2 にアップグレードして下さい*

  TLS 1.1/1.2 をアップグレードし、使用して下さい。 このソリューションの制限は ASA 5500-X ASA プラットフォームにだけ適用することです。 レガシー ASA プラットフォーム（ASA 5505 および ASA 5500 シリーズ）の暗号化ハードウェアは TLSv1.2 をサポートしま

せん。 その結果、これらのプラットフォームのための修正は実行不可能です。

プロトコル の 制限が原因で、SSLv3 または TLSv1.0 のためのソリューションがありません; ただし、ほとんどの現代ブラウザは軽減のさまざまな方法を設定しました。

- Cisco バグ ID CSCuc85781: *WebVPN クッキー無作為化*

TLSv1.2 をサポートしない ASA ソフトウェア バージョンに関しては、Cisco はリスクを軽減するためにクッキーをこの修正でランダムにしました。 これは完全に獣不正侵入を防ぎませんが、それらの軽減を助けます。

**ヒント**： 完全に獣脆弱性から保護される唯一の方法は TLSv1.2 を使用することです。 これは暗号に類似したです。 Cisco はより新しいコードのより新しく、より強い暗号を追加し続けより古い暗号は既知の問題があるかもしれません（RC4 のような）。 従って、Cisco はより新しいプロトコルおよび暗号に移動することを推奨します。