ASA BEAST 脆弱性ソリューション

内容

概要

このドキュメントでは、保護されているコンテンツに対して不正なユーザのアクセスを許してしまう Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアの脆弱性について説明します。この問題の回避策についても説明します。

問題

SSL/TLS(BEAST)に対するブラウザのエクスプロイトの脆弱性は、既知のプレーンテキスト攻撃を伴う暗号ブロックチェーン(CBC)暗号化モードでInitialization Vector(IV)チェーニングを介して保護されたコンテンツを効果的読に行います。

この攻撃では、広く使用されているTransport Layer Security Version 1(TLSv1)プロトコルの脆弱性を不正利用するツールが使用されます。この問題は、プロトコル自体に根ざしたものではなく、使用する暗号スイートに起因します。TLSv1およびセキュアソケットレイヤバージョン3(SSLv3)は、CBC暗号を優先します。この暗号では、Padding Oracle攻撃が発生します。

ユーザへの影響

SSL Pulse SSL実装調査では、Trustworthy Internet Movement(信頼できるインターネットの動作)により示されているように、SSLサーバの75 %以上がこの脆弱性の影響を受ける可能性があります。しかし、BEASTツールに関する物流はかなり複雑です。BEASTを使用してトラフィックを傍受するには、攻撃者がパケットを非常に迅速に読み込み、挿入できる必要があります。これは、BEAST攻撃の有効な標的を制限する可能性があります。たとえば、BEAST攻撃者は、WIFIホットスポットでランダムなトラフィックを効果的に捕捉したり、限られた数のネットワークゲートウェイですべてのインターネットトラフィックをボトルネックにすることができます。

解決方法

BEASTは、プロトコルによって使用される暗号の弱点を悪用したものです。CBC暗号に影響するため、この問題の最初の回避策は、代わりにRC4暗号に切り替えることでした。しかし、2013年

に発表されたRC4の主要なスケジューリングアルゴリズムの弱点は、RC4でさえ不適切な弱点を持っていたことを明らかにしています。

この問題を回避するために、シスコではASAに次の2つの修正を実装しています。

- Cisco Bug ID CSCts83720:*TLS 1.1/1.2へのアップグレード*

  TLS 1.1/1.2をアップグレードして使用します。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のみ適用されます。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をサポートしていません。そのため、これらのプラットフォームに対する修正は実行できません。

  プロトコルの制限により、SSLv3またはTLSv1.0のソリューションはありません。しかし、最近のほとんどのブラウザでは、さまざまな緩和方法が実装されています。

- Cisco Bug ID CSCuc85781:*WebVPN Cookieのランダム化*

  TLSv1.2をサポートしていないASAソフトウェアバージョンでは、リスクを軽減するために、シスコはこの修正でCookieをランダムに作成しました。これはBEAST攻撃を完全に防止するわけではありませんが、BEAST攻撃の軽減に役立ちます。

  ヒント:BEASTの脆弱性から完全に保護される唯一の方法は、TLSv1.2を使用することです。これは暗号に似ています。シスコは新しいコードで新しい強力な暗号を追加し続けます。古い暗号には既知の問題（RC4など）がある可能性があります。 したがって、新しいプロトコルと暗号に移行することを推奨します。