SSLv3 および TLSv1 プロトコルの CBC モードの脆弱性

目次

概要

この資料に Cisco E メール セキュリティ アプライアンス（ESA）の Cipher Block Chaining（CBC）モード暗号をディセーブルにする方法を記述されています。 セキュリティ監査/スキャンは ESA に Secure Sockets Layer（SSL）v3/Transport 層 セキュリティ（TLS）v1 プロトコル弱い CBC モード脆弱性があることを報告するかもしれません。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

この文書に記載されている情報は E メール セキュリティ（あらゆる修正）、Cisco ESA、およびバーチャル ESA のための AsyncOS に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

- Payment Card Industry Data Security Standard（PCI DSS）に準拠するには、CBC 暗号化を無効にする必要があります。
- セキュリティ監査/スキャンは、CBC モードの暗号化を使用した SSLv3/TLSv1 プロトコルに潜在的な脆弱性を確認しました。

  ヒント： SSL バージョン 3.0（RFC-6101）は古く、安全でないプロトコルです。 SSLv3 CVE-2014-3566 に、Padding Oracle On Downgraded Legacy Encryption（POODLE）攻撃として知られる脆弱性があります。Cisco Bug ID は CSCur27131 です。 推奨される解決策は、暗号化を変更する間 SSL v3 を無効にし、TLS のみを使用して、オプション 3（TLS v1）を選択することです。 詳細は、提供される Cisco Bug ID CSCur27131 を参照してください。

SSL v3 および TLS v1 プロトコルは HTTP や Lightweight ディレクトリ アクセス プロトコル（LDAP）などの他のプロトコルに整合性、信頼性、およびプライバシーを提供するために使用されます。 これらのプロトコルは、プライバシーのために暗号化を、信頼性のためにx509 証明書を、整合性のために一方向の暗号化機能を使用することで、これらのサービスを提供します。データを暗号化するために、SSL および TLS はブロック暗号を使用できます。ブロック暗号とは、元のデータの固定ブロックのみを同じサイズの暗号化されたブロックに暗号化できる暗号化アルゴリズムです。 これらの暗号は、同じ元のデータ ブロックに対しては同じ結果のブロックに常になることに留意してください。 出力の差を実現するために、暗号化の出力に対して、同じサイズの別のブロックを初期ベクトル（IV）として XOR 演算が行われます。 CBC は、最初のブロックに 1 つの IV を使用し、その後のブロックそれぞれに対し前のブロックの結果を使用して、ブロック暗号化の出力の差を実現します。

SSL v3 および TLS v1 の実装では、最初の IV を使用する 1 つの CBC セッションをトラフィック全体が共有するため、CBC モードの使用を選択することは適切ではありませんでした。 残りの IV は、前述したように、前のブロックの暗号化の結果です。 後続の IV は盗聴者が使用できます。 これにより、任意のトラフィックを（クライアントによって暗号化される）プレーン テキストのストリームに注入する機能がある攻撃者は、注入されたブロックに先行するプレーンテキストの推測を検証することができます。 攻撃者の予測が正しければ、暗号化の出力は 2 つのブロックで同じです。

エントロピーが低いデータの場合は、比較的少ない試行でプレーンテキスト ブロックを推測することが可能です。 たとえば、1000 通りの可能性があるデータの場合、試行回数は 500 にすることができます。

要件

これを悪用するには、あるいくつかの要件を満たす必要があります。

1. SSL/TLS 接続で、DES や AES などの CBC モードを使用するブロック暗号化方式のいずれかが使用されている必要があります。 RC4 などのストリーム暗号を使用したチャネルは欠陥の影響を受けません。 SSL/TLS 接続の大部分で RC4 が使用されている。
2. 脆弱性は、SSL/TLS 接続でデータを傍受し、その接続で新しいデータをアクティブに送信する攻撃者によってのみ悪用されます。 欠陥を悪用されることで SSL/TLS 接続が終了します。 攻撃者は、メッセージを復号化するために十分なデータが収集されるまで、新しい接続を監視し使用し続ける必要があります。

3. 接続が毎回終了するので、SSL/TLS クライアントはメッセージの複合に十分な長さの SSL/TLS チャネルを再確立し続けることが可能である必要があります。
4. アプリケーションは作成する各 SSL/TLS 接続で同じデータを再送信する必要があり、リスナーはそのデータをデータ ストリームに位置付ける必要があります。 ログインするための一定のメッセージがある IMAP/SSL のようなプロトコルはこの要件を満たしています。 一般的な Web ブラウジングは満たしていません。

脅威

CBC の脆弱性は、TLS v1 の脆弱性です。 この脆弱性は、2004 年前半から存在が確認され、TLS v1.1 および TLS v1.2 の以降のバージョンで解決されています。

AsyncOS 9.6 for Email Security 以前は、ESA は TLS v1.0 および CBC モードの暗号を使用します。 AsyncOS 9.6 リリース以降、ESA には TLS v1.2 が導入されました。 ただし、CBC モードの暗号は無効にでき、欠陥の影響を受けない RC4 の暗号のみを使用できます。

また、SSLv2 が有効になっている場合、この脆弱性に対し誤検出を引き起こす場合があります。 SSL v2 を無効にすることは非常に重要です。

解決策

RC4 の暗号のみを有効なままにするために、CBC モードの暗号を無効にします。 TLS v1、または TLS v1/TLS v1.2 のみを使用するようにデバイスを設定します。

1. CLI にログインします。
2. コマンド **sslconfig** を入力します。
3. コマンド **GUI** を入力します。
4. 「TLS v1」のオプション番号 3、または AsyncOS 9.6 にリストされている「TLS v1/TLS v1.2」のとおりに選択します。
5. 次の暗号を入力します。`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. 次のコマンドを入力します。 **INBOUND**:
7. 「TLS v1」のオプション番号 3、または AsyncOS 9.6 にリストされている「TLS v1/TLS v1.2」のとおりに選択します。
8. 次の暗号を入力します。`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
9. コマンド **OUTBOUND** を入力します。
10. 「TLS v1」のオプション番号 3、または AsyncOS 9.6 にリストされている「TLS v1/TLS v1.2」のとおりに選択します。
11. 次の暗号を入力します。`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
12. ホスト名のプロンプトに戻るまで [ENTER] を押します。
13. コマンド **commit** を入力します。
14. 変更のコミットを完了します。

ESA は RC4 で暗号化を行う TLS v1 または TLSv1/TLS v1.2 のみをサポートし、CBC フィルタを許可しないように設定されます。

次に、RC4:-SSLv2.を設定するときに使用される暗号リストを示します。 リストには CBC モー

ドの暗号はないことに注意してください。

```
ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
EXP-ADH-RC4-MD5 SSLv3 Kx=DH(512) Au=None Enc=RC4(40) Mac=MD5 export
EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
```

この不正利用はその複雑性と要件から悪用の心配は低い一方で、これらの手順を実行することで、考えられる不正利用の阻止および厳密なセキュリティ スキャンの実行にとって大きなセーフガードとなります。

関連情報

- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- テクニカルサポートとドキュメント - Cisco Systems