

# SSL v3 および TLS v1 プロトコル弱い CBC モード脆弱性

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[要件](#)

[脅威](#)

[解決策](#)

[関連情報](#)

## 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 ) モード暗号を無効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。

Attention ( 注意 ) : E メール セキュリティ用の AsyncOS のより古いコードを実行する場合、バージョン 11.0.3 または それ 以降にアップグレードすることを推奨します。最新バージョンおよび情報に関する [Cisco E メール セキュリティ リリース ノート](#) を検討して下さい。アップグレードの詳細事項をまたは無効になる暗号必要とする場合、[サポート ケース](#) をオープンして下さい。

## 前提条件

### 要件

このドキュメントに関しては個別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。

本書の情報は、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、初期 ( デフォルト ) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

## 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](#) ) は廃止および不安定なプロトコルです。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。出力の違いを実現させるために、暗号化の出力は初期化ベクトル ( iv ) と言われる同じサイズの更に別のブロックとの XORed です。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。攻撃者の推測が正しい場合、暗号化の出力は 2 つのブロックのため同じです。

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 接続は CBC モードを使用する DES または AES のようなブロック暗号化暗号の 1 つを使用する必要があります。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。欠陥の不正利用は SSL/TLS 接続を終えます。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 チャン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。この脆弱性は早い 2004 年以降のプロシージャにあり、TLS v1.1 および TLS v1.2 の以降のバージョンで解決されました。

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 のリリースによって、ESA は TLS v1.2 を導入します。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

Attention (注意) : E メールセキュリティ用の AsyncOS のより古いコードを実行する場合、バージョン 11.0.3 またはそれ以降にアップグレードすることを推奨します。最新バージョンおよび情報に関する [Cisco E メールセキュリティリリースノート](#) を検討して下さい。アップグレードの詳細事項をまたは無効になる暗号必要とする場合、[サポートケース](#) をオープンして下さい。

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」のとおりを選択します。

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」のとおりを選択します。

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」のとおりを選択します。

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.を設定するときを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
```

このエクスプロイトが複雑な状況および必要条件による非常に低い問題不正利用するである間、これらのステップのパフォーマンスは可能性のある エクスプロイトの防止のための大きい安全対策、また厳密なセキュリティ スキャンを渡すためにです。

## 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](#)