TKIP暗号化の脆弱性に対するシスコの対応

Informational

アドバイザリーID : cisco-sa-20081121-wpa
初公開日 : 2008-11-21 16:00
バージョン 1.0 : Final
回避策 : No Workarounds available
Cisco バグ ID :

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

最近、テクノロジー業界やその他の報道機関が、Temporal Key Integrity Protocol(TKIP)のセキュリティ脆弱性に関する記事を発表しました。TKIPは、Wired Equivalency Protocol(WEP)でセキュリティの脆弱性が発見されてから開発されました。このプロトコルは、高度暗号化規格(AES)をサポートできないワイヤレスデバイスのWEPにおけるワイヤレスセキュリティの制限に対処するための一時しのぎのメカニズムとして開発されました。

TKIPは、Wi-Fi Protected Access(WPA)仕様の最初のバージョンに必須の暗号スイートであり、Wi-Fi Protected Access version 2(WPA2)標準のオプションです。

追加情報

TKIPには、特定の状況で攻撃者がパケットを復号化できる脆弱性があります。これはキー回復攻撃ではありません。攻撃者は、パケットの認証に使用されるキーだけを回復できますが、データの暗号化と難読化に使用されるキーは回復できません。復元されたキーを使用すると、キャプチャされたパケットだけが、最大7回の試行という限られた期間で偽造される可能性があります。攻撃者は一度に1つのパケットだけを復号化できます。現在は、12 ~ 15分ごとに1パケットのレートで復号化できます。さらに、パケットはワイヤレスアクセスポイント(AP)からクライアント（単方向）に送信された場合にのみ復号化できます。これらの攻撃の影響を受けるのは、暗号化メカニズムとしてTKIPを使用するように設定されたデバイスだけです。AES-CCMP暗号スイートと共にWPA2を使用するお客様は、これらの攻撃に対して脆弱ではありません。

AESはより安全な暗号化アルゴリズムであり、米国政府が機密扱いではないデータと機密扱いのデータの両方を暗号化することは許容できると考えられています。現時点では、AES暗号化キーを突破する成功した攻撃はありません。AESは現在の最高暗号化規格であり、WEPに代わるものです。そのため、可能な限りWPA2をAESと組み合わせて使用することをお勧めします。その前身であるWPAは暫定プロトコルでした。最近のワイヤレスデバイスとクライアントの大部分は、

AES暗号化規格をサポートしています。

注：WPA2対応クライアントのリストについては、http://www.wi-fi.orgを参照してください。

ハードウェアの老朽化やドライバの互換性がないことが原因で、クライアントがAESによるWPA2をサポートしていない場合、VPNは無線クライアント接続を保護するための次に最適なソリューションです。複数のSSIDとVLANを使用したネットワークセグメンテーションと組み合わされたVPNは、多様なクライアントを持つネットワークに堅牢なソリューションを提供します。IP Security(IPSec)VPNとSecure Sockets Layer(SSL)VPNは、WPA2と同じレベルのセキュリティを提供します。

AESを使用したWPA2が使用できない場合は、次の回避策と緩和策を使用できます。

回避策と緩和策

この問題を軽減するには、ペアワイズキーをより頻繁に回すことを推奨します。キー再生成の間隔を120秒にすることを推奨しましたが、ほとんどの環境では、攻撃者が部分キーの回復に8分以上かかる必要があるため、300秒の回転間隔を使用するだけで十分です。この間隔を長くしても十分であり、RADIUSサーバの負荷が軽減される可能性があります。

注意：EAPを使用している場合は、キーローテーション間隔を短くすると、RADIUSサーバの負荷が増加します。

Autonomous APでは、**dot1x timeout reauth-period <*nSeconds*>**コマンドを使用して、キーの回転間隔を変更できます。

注：このコマンドは、設定に応じて、APごと、Wireless Domain Services（WDS；無線ドメインサービス）ごと、またはRADIUSサーバから提供される方法でグローバルに使用できます。

ワイヤレスLANコントローラ(WLC)のWebコンソールで、[WLANs] > [Advanced] > [Enable Session Timeout] に移動します。または、**config wlan session-timeout <*wlanID*> <*nSeconds*>**コマンドラインインターフェイス(CLI)コマンドを使用して、キーの回転間隔を変更できます。

WMMの無効化は、シスコ製品に対する実行可能な回避策として、現在も調査中です。

Wi-Fi Protected Access(WPA)に組み込まれているMessage Integrity Check(MIC)エラーは、必ずしも攻撃を示すものではありません。実際には、Cisco 7920電話など、さまざまなクライアントで、通常の動作でMIC工ラーが発生することが知られています。ただし、慎重に実行されたこの攻撃のインスタンスは、1分に1回未満の割合でMICエラーを生成し、AP対策のトリガーを防ぎます。APの対応策が有効になっている場合に表示されるワイヤレスLANコントローラ(WLC)システムメッセージの例を次に示します。

```
The AP '00:0b:85:67:6b:b0' received a WPA MIC
     error on protocol '1' from Station '00:13:02:8d:f6:41'.
```

```
Counter measures have been activated and traffic has
been suspended for 60 seconds.
```

このエラーは、ネットワーク内の誰かが元のクライアントから送信されたメッセージを再生しようとしているか、クライアントに障害があることを示している可能性があります。クライアントで MIC チェックが繰り返し失敗すると、コントローラは WPA プロトコルの要件に従って、その WLAN を 60 秒間ディセーブルにします。これにより、暗号化スキームへの潜在的な攻撃が防止されます。これらの MIC エラーを、コントローラでオフにすることはできません。詳細については、次のリンクにある『ワイヤレスLANコントローラ(WLC)のエラーメッセージとシステムメッセージに関するFAQ』を参照してください。

http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008082c464.shtml

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の説明も含まれています。すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20081121-wpa

改訂履歴

バージョン	説明	セクション	日付
リビジョン 1.0	初回公開リリース		2008年11月21日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。