GETVPN の Perfect Forward Secrecy

グループメンバー（GM）が侵害された場合、攻撃者は保存された長期キーとメッセージにアクセスする可能性があります。GETVPN の Perfect Forward Secrecy（PFS）により、攻撃者はキーとメッセージを使用して過去または将来のセッションのキーを取得することができなくなります。そのため、攻撃者は、侵害されたトラフィック暗号化キー（TEK）を使用して現在のセッションの通信を復号することは可能ですが、録音された通信や将来の通信は復号できません。

GETVPN の PFS に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : GETVPN の PFS* に関する機能情報

機能名	リリース	機能情報
GETVPN の Perfect Forward Secrecy	Cisco IOS XE Gibraltar 16.12.1	次のコマンドが導入または変更されました。**show crypto gkm feature pfs**、**pfs**、**show crypto gdoi**、および **client pfs**。

GETVPN の PFS に関する情報

GETVPN の PFS の概要

仮に、デバイスが侵害され、攻撃者が、デバイスに保存されている長期キーにアクセスしたとします。Perfect Forward Secrecy（PFS）では、攻撃者が長期キーを使用してキーを取得し、過去のセッションの記録された通信を復号することを防止します。関連するセキュリティ対策に、「Perfect Backward Secrecy（PBS）」と呼ばれるものがあります。PBS では、攻撃者が長期キーを使用してキーを取得し、将来のセッションの通信を復号することを防止します。

GM が侵害された場合、攻撃者は保存された長期キーとメッセージにアクセスする可能性があります。それにより、攻撃者は、Diffie-Hellman（DH）の結果および登録メッセージ、またはキー暗号化キー（KEK）と過去のキー再生成メッセージを取得する可能性があります。GETVPN の PFS では、攻撃者は、キーとメッセージを使用して過去のセッションの TEK を取得することができません。さらに、攻撃者は、KEK を使用して将来のキー再生成メッセージを復号できないため、将来のセッションの TEK を取得できません。そのため、攻撃者は、現在のセッションの TEK にのみアクセスできます。キーが侵害されても、記録された通信や将来の通信は安全なままです。

GETVPN の PFS には、次の変更点が含まれています。

- キー再生成プロセスが変更されています。GM 登録メカニズムは変更されていません。
- GETVPN の PFS を有効にすると、GM-KS IKEv2 チャネルのデフォルトのライフタイムが 1 日から 600 秒に変更されます。

  ただし、カスタマイズされたライフタイムを設定している場合は、GETVPN の PFS を有効にした後もライフタイムは変更されません。
- GETVPN の PFS をサポートするキーサーバー（KS）とグループメンバー（GM）には、新しいバージョン番号があります。このバージョン番号は、サードパーティの GM との後方互換性およびインタラクションをサポートします。

GETVPN の PFS に関する制約事項

- キーサーバー（KS）とグループメンバー（GM）は、IKEv2 プロトコルを使用して通信する必要があります。KS と GM が IKEv1 プロトコルを使用して通信する場合、GETVPN の PFS はサポートされません。
- COOP 内のすべての KS で PFS を有効にしてください。GM では、PFS はデフォルトで有効になっています。
- スケジュールされたキー再生成と手動でトリガーされたキー再生成の両方によって、GM が KS に再登録されます。この再登録により、特に大規模な場合に、KS で顕著なオーバーヘッドが発生する可能性があります。

- キー再生成を強制すると、GM 間のキーの不一致が原因でトラフィックが失われる可能性があります。
- RSA キーサイズが 4096 の場合は、キーのサイズが大きいために、暗号化エンジンによるキー再生成の署名にかなりの時間がかかります。キー再生成の署名中に受信した登録要求が多すぎると、暗号化エンジンが過負荷状態になる可能性があります。オーバーロードされた暗号化エンジンは、次のエラーメッセージをログに記録します。

```
%ACE-3-TRANSERR: IOSXE-ESG(9): IKEA trans 0x11A8; opcode 0x23; param 0x0; error 0xC;
 retry cnt 0
```

このエラーメッセージは、4096 の RSA キーサイズを使用しており、100 を超える GM があり、PFS が有効になっている GETVPN 展開において、より頻繁に表示される可能性があります。頻度が増加するのは、PFS が有効になっている場合、キー再生成のたびに再登録がトリガーされ、100 を超える GM では、暗号化エンジンがキー再生成の署名中に複数の登録要求を受信する可能性が高くなり、過負荷状態になる可能性があるためです。

同様に、そのような展開では、**crypto gdoi ks rekey replace-now** コマンドを繰り返し実行すると、このコマンドによってトリガーされる登録要求のために、このエラーメッセージがより頻繁に表示される可能性があります。

PFS が有効になっている GETVPN 展開では、2048 の RSA キーサイズを使用することをお勧めします。キー再生成メッセージには TEK/KEK キーが含まれないため、4096 の RSA キーサイズを使用する必要はありません。

変更されたキー再生成プロセス

GETVPN の PFS は、攻撃者が侵害された GM からの KEK を使用して過去または将来のキー再生成メッセージを復号できないようにします。そのため、攻撃者は、過去または将来の KEK や TEK を取得できません。この目的のために、GETVPN の PFS は、キー再生成メカニズムを変更して、キー再生成メッセージに KEK または TEK が含まれないようにします。キー再生成メッセージの内容は、キー再生成のタイプによって異なります。

スケジュールされたキー再生成

1. KEK または TEK のキー再生成タイマーが切れると、KS はそれぞれ新しい KEK または TEK を生成します。
2. KS は、キー再生成メッセージの GSA ペイロードにプライベート属性を設定し、現在の KEK でメッセージを暗号化します。キー再生成メッセージには、新しい KEK または TEK は含まれません。KS は、GM にキー再生成メッセージを送信します。
3. GM は、キー再生成メッセージを受信し、現在の KEK を使用してメッセージを復号します。GM は、スケジュールされたキー再生成を識別し、0 ～ 6 秒の範囲のランダムな時間間隔で再登録タイマーを開始します。
4. 再登録タイマーが切れると、GM は KS への再登録を開始します。
5. 再登録後、KS は、IKEv2 チャネルを介して KEK または TEK を GM に送信します。

6. 新しい KEK を受信すると、GM は、古い KEK を新しい KEK に置き換えます。
7. 新しい TEK を受信すると、GM は、TEK のアクティブ化時間遅延（ATD）を確認します。ATD が 0 以外の場合、GM は、データプレーンに TEK をインストールする前にタイマーを開始して ATD を適用します。

   ATD は、KS で次のように計算されます。

   1. 長い SA ライフタイムが設定されている場合、ATD タイマーは、次のように計算される秒単位の値に初期化されます。ATD =（古い TEK の残りのライフタイム）-（古い TEK の残りのライフタイムの 1%）- 75

      新しい TEK は、（古い TEK の残りのライフタイムの 1%）時にロールオーバーされます。

   2. 長い SA ライフタイムが設定されていない場合、ATD タイマーは、次のように計算される秒単位の値に初期化されます。ATD =（古い TEK の残りのライフタイム）- 75

      新しい TEK は、古い TEK の有効期限が切れる 30 秒前にロールオーバーされます。

同期キー再生成

1. KS は、pseudoTimeStamp（PST）値のみを含むキー再生成メッセージを GM に送信します。

   このメッセージに KEK または TEK は含まれません。
2. キー再生成メッセージを受信すると、GM は、疑似時間値を更新し、再登録をトリガーしません。KS から受信した pseudoTimeStamp 値と GM で設定された 時間ベースアンチリプレイ（TBAR）ウィンドウに応じて、GM が Syslog メッセージを生成する場合があります。

手動でトリガーされるキー

1. **crypto gdoi ks** または **clear crypto gdoi ks members** を使用してキー再生成動作をトリガーすると、KS は、キー再生成タイプに基づいて GAP/DELETE ペイロードを送信します。
   - ポリシー変更のないキー再生成メッセージ

表 *2*：ポリシー変更のないキー再生成メッセージの *GAP/DELETE* ペイロード

Type	KEK	TEK	キー再生成のプライベート属性	KD	GAP	DELETE
`crypto gdoi ks rekey`	非対応	非対応	非対応	非対応	非対応	非対応
`crypto gdoi ks rekey replace-now`	非対応	非対応	はい	非対応	ATD 1 秒	未対応
`clear crypto gdoi ks members`	非対応	非対応	非対応	非対応	ATD TEK の 5%	対応

Type	KEK	TEK	キー再生成のプライベート属性	KD	GAP	DELETE
clear crypto gdoi ks members now	非対応	非対応	はい	非対応	ATD 1 秒	対応

- ポリシー変更のある再生成メッセージ

表 *3*：ポリシー変更のあるキー再生成メッセージの *GAP/DELETE* ペイロード

Type	KEK	TEK	キー再生成のプライベート属性	KD	GAP	DELETE
crypto gdoi ks rekey	非対応	非対応	はい	非対応	ATD TEK の 5%	未対応
crypto gdoi ks rekey replace-now	非対応	非対応	はい	非対応	ATD 1 秒	未対応
clear crypto gdoi ks members	非対応	非対応	非対応	非対応	ATD TEK の 5%	対応
clear crypto gdoi ks members now	非対応	非対応	はい	非対応	ATD 1 秒	対応

2. キー再生成メッセージを受信した GM は、KS への再登録を開始します。
3. 再登録の一環として、KS は、IKEv2 チャネルを介して KEK または TEK を GM に送信します。
4. GM は、古いキーのライフタイムを、KS から送信されたアクティブ化時間遅延（ATD）値に設定します。ATD の後、GM は、古いキーを削除し、新しいキーをインストールします。

Suite B のサポート

GM の初回登録時に、KS は、一意の送信者識別子（SID）と初期化ベクトル（IV）範囲を GM に割り当てます。GM がキー再生成メッセージに応答して KS に再登録する場合、GM は、KS が登録時に割り当てた SID を提供します。KS は、新しい SID または初期化ベクトル（IV）範囲を GM に割り当てません。

GETVPN の PFS の KS バージョンおよび GM バージョン

Cisco IOS XE Gibraltar 16.12.1 以降のリリースが GM にインストールされている場合、GETVPN の PFS はデフォルトで有効になります。コマンドラインインターフェイスを使用して、GETVPN の PFS を無効にできます。GM のバージョンは、次の表に示すように、PFS が有効になっているかどうかによって異なります。

	Suite B サポートなし	Suite B サポートあり	ASR 1000 シリーズ
PFS が無効	16	17	19
PFS が有効	21	22	20

Cisco IOS XE Gibraltar 16.12.1 以降のリリースが KS にインストールされている場合、GETVPN の PFS はデフォルトで無効になり、KS のバージョンは 1.0.18 です。CLI を使用して、GETVPN の PFS を有効にできます。GETVPN の PFS が有効になっている場合、KS のバージョンは 1.0.23 です。すべての連携 KS で GETVPN の PFS を有効にします。

KS は、GM のバージョンに基づいて、キー再生成メッセージを GM に送信します。

- GETVPN の PFS が無効になっており、1.0.17 や 1.0.19 などのバージョン番号を送信する GM に対して、KS は、KEK または TEK を含むキー再生成メッセージを送信します。

  KS は、GETVPN の PFS が無効になっている GM およびシスコ以外の GM に、KEK または TEK を含むキー再生成メッセージを送信します。GETVPN の PFS が無効になっている GM は、1.0.17 や 1.0.19 などのバージョン番号を KS に送信します。シスコ以外の GM は、KS に不明なバージョン番号を送信します。

- KS は、GETVPN の PFS が有効になっている GM に、KEK または TEK を含まない、変更されたキー再生成メッセージを送信します。GETVPN の PFS が有効になっている GM は、1.0.20 や 1.0.22 などのバージョン番号を送信します。

GETVPN の PFS のKS および GM の更新

GETVPN の PFS を有効にするには、ネットワーク内のすべての KS および GM で PFS を有効にします。GM で GETVPN の PFS を有効にしていない場合、GM が侵害されると、侵害されたキーにより、ネットワーク全体のセキュリティが妨げられる可能性があります。

次のように、ネットワーク内の KS をアップグレードします。

（注） KEK と TEK の有効期限が切れるまでに十分な時間がある間に KS をアップグレードすることをお勧めします。

1. セカンダリ KS をアップグレードし、COOP の選択が完了するまで待ちます。
2. COOP の各セカンダリ KS について、手順 1 を繰り返します。

   セカンダリ KS が再起動してプライマリ KS と同期し、セカンダリ KS の役割を担います。
3. プライマリ KS をアップグレードします。

   セカンダリ KS の 1 つが新しいプライマリ KS として選択されます。アップグレードされた KS が再起動し、セカンダリ KS の役割を担います。

4. すべての KS で PFS を有効にします。

アップグレード後、KS は、GM が送信するバージョン番号に基づいてキー再生成メッセージを送信します。GM バージョン番号に基づいて、KS は、KEK または TEK を含むキー再生成メッセージか、KEK または TEK を含まない変更されたキー再生成メッセージを送信します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。