既存の暗号化設定でペイロード暗号化イメージを使用しない場合のセキュリティ上の問題の識別と緩和

Informational

アドバイザリーID : cisco-sa-npe-hardening-Dkel83jP
初公開日 : 2023-01-18 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

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアイメージには、通常の**universalk9**イメージとNo Payload Encryption(NPE)**universalk9_npe**イメージの2つのタイプがあります。NPEイメージは、プラットフォームが強力なペイロード暗号化をサポートしないことを必要とする一部の国の輸入要件を満たすために導入されました。そのため、NPEイメージでは、IPsec VPNやSecure Unified Communicationsなど、特定の暗号化機能がサポートされていません。

その結果、NPEイメージを実行している場合、CLIパーサーはこれらの機能に関連するコマンドをサポートしなくなります。このようなコマンドがCLIで入力されると、パーサーは無効なコマンドを含むエラーメッセージで応答します。これは予期された動作ですが、状況によっては、暗号化設定のリークにつながる可能性があります。

次の一連のイベントによって、このようなリークが発生する可能性があります。

1. デバイスがブートされ、**universalk9**イメージがロードされます。次に、秘密または重要な資料の設定を必要とする1つ以上の機能を使用してデバイスを設定します。
2. デバイス上のイメージが**universalk9_npe**イメージに置き換えられ、以前に設定されたシークレットやキーマテリアルを削除せずにリブートされます。

次に、**startup-config**に存在する既存の設定コマンドが解析されますが、設定された強力なペイロード暗号化機能に関連する設定コマンドは認識されず、対応するエラーメッセージがコンソールに表示されます。特定のシナリオでは、インターネットキーエクスチェンジ(IKE)の事前共有キーなどの機密情報がエラーメッセージに含まれる場合があります。

このアドバイザリは、次のリンクより確認できます。

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-npe-hardening-DkeI83jP

脆弱性のある製品

この問題は、Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアを実行し、強力なペイロード暗号化機能が有効になっているシスコ製品に影響を与えました。強力なペイロード暗号化機能には、次のものがあります。

- インターネットプロトコルセキュリティ(IPsec)VPN
- LoRaWAN
- Media Access Control Security(MACsec)
- SD-WAN
- Secure StackWise Virtual
- セキュアなユニファイドコミュニケーション
- SSL VPN
- Wireless Personal Area Network(WPAN)

脆弱性を含んでいないことが確認された製品

このアドバイザリの「脆弱性が存在する製品」セクションに記載されている製品のみが、この問題の影響を受けることが確認されています。

出典

この問題を報告していただいたE.ON PentestingのDaniel Szameitat氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-npe-hardening-DkeI83jP

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	-	Final	2023年1月18日

利用規約

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。