複数のシスコ製品におけるConfidential Information Decryption Man-in-the-Middle脆弱性

Medium

アドバイザリーID : cisco-sa-20151125-ci　CVE-2015-6358
初公開日 : 2015-11-25 21:30
最終更新日 : 2016-09-20 21:24
バージョン 1.4 : Final
CVSSスコア : 5.0
回避策 : No workarounds available
Cisco バグ ID : CSCuw47040 CSCuw47061 CSCuw46677 CSCuw46610 CSCuw46654 CSCuw46665 CSCuw47028 CSCuw46620 CSCuw47005 CSCuw47048 CSCuw46672 CSCuw46682 CSCuw90875 CSCuw46705 CSCuw46716 CSCuw46979 CSCuw46637 CSCuw90869 CSCuw90913 CSCuw90899 CSCuw90860 CSCuw90881

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

複数のシスコ製品の暗号化実装における脆弱性により、認証されていないリモートの攻撃者が、該当デバイスのファームウェアに組み込まれたハードコードされた証明書とキーを使用できる可能性があります。

この脆弱性は、該当するアプライアンス内で一意のキーと証明書が生成されないことに起因します。攻撃者は、静的な情報を使用して中間者攻撃を行い、ユーザ接続の機密情報を復号化することで、この脆弱性を不正利用する可能性があります。

これは、デバイスにアクセスしようとするクライアントに対する攻撃であり、デバイス自体を危険にさらすものではありません。この問題を不正利用するには、攻撃者は公開キーと秘密キーのペアだけでなく、クライアントとサーバ間のトラフィックを監視し、トラフィックを代行受信し、攻撃者自身のトラフィックを変更または注入できる権限を持つネットワーク上の位置も必要です。この脆弱性に対処する回避策はありません。

シスコでは、本脆弱性に対処するソフトウェア アップデートをリリースしていません。

このアドバイザリは次のリンクで確認できます。

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151125-ci

該当製品

脆弱性のある製品

次の製品に脆弱性が存在します。

- RV320 デュアル ギガビット WAN VPN ルータ
- RV325 デュアル ギガビット WAN VPN ルータ
- RVS4000 4ポートギガビットセキュリティルータ – VPN
- WRV210 Wireless-G VPNルータ – RangeBooster
- WAP4410N Wireless-Nアクセスポイント – PoE/Advanced Security
- WRV200 Wireless-G VPNルータ – RangeBooster
- WRVS4400N Wireless-Nギガビットセキュリティルータ – VPN V2.0
- WAP200 Wireless-Gアクセスポイント – PoE/Rangebooster
- WVC2300 Wireless-Gビジネスインターネットビデオカメラ – オーディオ
- PVC2300ビジネスインターネットビデオカメラ – 音声/PoE
- SRW224P 24ポート10/100 + 2ポートギガビットスイッチ – WebView/PoE
- WET200 Wireless-Gビジネスイーサネットブリッジ
- WAP2000 Wireless-Gアクセスポイント – PoE
- WAP4400N Wireless-Nアクセスポイント – PoE
- RV120W Wireless-N VPNファイアウォール
- RV180 VPNルータ
- RV180W Wireless-N多機能VPNルータ
- RV315W Wireless-N VPNルータ
- Small Business SRP520モデル
- Small Business SRP520-Uモデル
- WRP500 Wireless-ACブロードバンドルータ（2電話ポート）
- SPA400インターネットテレフォニーゲートウェイ（4つのFXOポート）
- RTP300ブロードバンドルータ
- RV220Wワイヤレスネットワークセキュリティファイアウォール

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

回避策

この脆弱性に対処する回避策はありません。緩和策として、SSHおよびHTTPSを介したデバイスの管理インターフェイスへのアクセスを、既知の信頼できるIPアドレスのサブセットに制限する必要がある場合があります。

修正済みソフトウェア

Cisco Bugsで修正されたソフトウェアに関する情報は、 Cisco Bug Search Toolで検索できます。

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成は新規リリースでも継続して適切なサポートが受けられることを確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

- RV320デュアルギガビットWAN VPNルータ：ファームウェアバージョン1.3.1.12が利用可能
- RV325デュアルギガビットWAN VPNルータ：ファームウェアバージョン1.3.1.12が利用可能
- RVS4000 4ポートギガビットセキュリティルータ – VPN：修正は提供されません
- WRV210 Wireless-G VPNルータ – RangeBooster：修正は提供されません
- WAP4410N Wireless-Nアクセスポイント – PoE/Advanced Security：修正は提供されません

- WRV200 Wireless-G VPNルータ – RangeBooster：修正は提供されません
- WRVS4400N Wireless-Nギガビットセキュリティルータ – VPN V2.0：修正は提供されません
- WAP200 Wireless-Gアクセスポイント – PoE/Rangebooster：修正は提供されません
- WVC2300 Wireless-Gビジネスインターネットビデオカメラ – 音声：修正プログラムは提供されません
- PVC2300 Business Internet Video Camera - Audio/PoE：修正は提供されません
- SRW224P 24ポート10/100 + 2ポートギガビットスイッチ – WebView/PoE：修正は提供されません
- WET200 Wireless-Gビジネスイーサネットブリッジ：修正は提供されません
- WAP2000 Wireless-Gアクセスポイント – PoE：修正は提供されません
- WAP4400N Wireless-Nアクセスポイント – PoE：修正は提供されません
- RV120W Wireless-N VPNファイアウォール：修正は提供されません
- RV180 VPNルータ：修正は提供されません：修正は提供されません
- RV180W Wireless-N多機能VPNルータ：修正プログラムは提供されません
- RV315W Wireless-N VPNルータ：修正プログラムは提供されません
- Small Business SRP520モデル：修正プログラムは提供されません
- Small Business SRP520-Uモデル：修正プログラムは提供されません
- WRP500 Wireless-ACブロードバンドルータ：Engineering Special(ES)で修正が解決されました。詳細については、Cisco TACにお問い合わせください。

・ SPA400インターネットテレフォニーゲートウェイ（4つのFXOポートを搭載）：修正は提供されません。
・ RTP300ブロードバンドルータ：修正は提供されません
・ RV220Wワイヤレスネットワークセキュリティファイアウォール：修正は提供されません

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team(PSIRT)は、このアドバイザリに記載されている脆弱性が、SEC Consult Vulnerability LabのStefan Viehböck氏によって公開されていることを認識しています。Cisco PSIRTでは、この脆弱性の不正利用は確認していません。

出典

シスコは、この脆弱性を発見し、報告していただいたSEC Consult Vulnerability LabのStefan Viehböck氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151125-ci

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.4	修正済みソフトウェアを更新し、Engineering Special(ES)に関する情報を追加。	修正済みソフトウェア	Final	2016年9月20日
1.3	修正済みソフトウェアを更新し、新しいソフトウェアアップデートに関する情報を追加。	修正済みソフトウェア	Final	2016年9月13日
1.2	修正が提供される時期を示すために該当製品を更新。	該当製品	Final	2016 年 1 月 21 日
1.1	概要、エクスプロイト事例と公表、回避策のセクションを更新して詳細を明確にしました。	概要、不正利用事例および公式発表、回避策	Final	2015-November-26
1.0	初版リリース	—	Final	2015-

バージョン	説明	セクション	ステータス	日付
				November-25

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。