Cisco Application Policy Infrastructure Controller エンタープライズ モジュールにおける不正アクセスの脆弱性

High

アドバイザリーID : cisco-sa-20171101-apicem

初公開日 : 2017-11-01 16:00

バージョン 1.0 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCve89638

CVE-2017-12262

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 Application Policy Infrastructure Controller エンタープライズ モジュール（APIC EM）のファイアウォール設定内の脆弱性により、近接する未認証の攻撃者が、デバイスの内部ネットワークのみで利用できるサービスに対して特権的にアクセスできる可能性があります。

この脆弱性は、デバイス上のファイアウォール ルールの誤りに起因するものです。 誤設定により、デバイスのパブリック インターフェイスに送られたトラフィックが APIC EM の内部仮想ネットワークに転送される可能性があります。 該当の APIC EM のパブリック インターフェイスが存在しているネットワークに論理的に近接する攻撃者がこの動作を利用して、内部ネットワークでリスニングしているサービスに対し、昇格された特権でアクセスできる可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-apicem

該当製品

脆弱性のある製品

この脆弱性は、バージョン 1.5 より前の Cisco Application Policy Infrastructure Controller エンタープライズ モジュールを実行している仮想デバイスまたはアプライアンスに影響します。

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。

詳細

セキュリティ侵害の痕跡

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この脆弱性は Cisco APIC-EM リリース 1.5 以降で修正されています。

ソフトウェアは Cisco.com の Software Center から**ダウンロード > ホーム > 製品 > クラウドおよびシステム管理 > ポリシーおよび自動化コントローラ > Application Policy Infrastructure Controller エンタープライズ モジュール (APIC-EM) へのによって > APIC-EM ソフトウェア Updates-1.5** ナビゲート ダウンロードすることができます

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

この脆弱性は、MWR InfoSecurity の Georgi Geshev 氏によってシスコに報告されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-apicem

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017 年 11 月 1 日

利用規約