Cisco Application Policy Infrastructure Controller カスタム バイナリの特権昇格の脆弱性

High

アドバイザリーID : cisco-sa-20170816-apic2

初公開日 : 2017-08-16 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCvc96087

CVE-2017-6768

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(APIC) デバイスのブート時にインストールされる特定の実行可能なシステム ファイルのビルド手順における脆弱性により、認証済みのローカル攻撃者に *ルート レベル*の権限を付与する恐れがあります。

この脆弱性は、ロードするライブラリを正しく検証せず関連検索パスを使用してビルドされたカスタム実行可能なシステム ファイルが原因です。 攻撃者はこの脆弱性を悪用して、デバイス認証し、権限レベルを昇格できる悪意のあるライブラリを読み込みます。 不正利用に成功すると、攻撃者は *ルート レベル*の権限を取得し、デバイスを完全に制御できるようになります。 攻撃者は、デバイスにログインするための有効なユーザー認証情報を有している必要があります。

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-20170816-apic2

該当製品

脆弱性のある製品

この脆弱性は、最初の正式リリースまでの間ソフトウェア リリース 1.0 (1e) を実行している場合に Cisco APIC に影響します。 該当するソフトウェア リリースについては、このアドバイザリの「修正済みソフトウェア」の項を参照してください。

APIC のどのリリースがデバイス上で実行されているかを検証するには、管理者は CLI コマンド **show version** を使用することができます。 次の例は、ソフトウェア リリース 1.2 (3m) を実行しているデバイスのコマンドの出力です。 :

```
APIC# show version Role        Id          Name                      Version
---------- ---------- ----------------------- ------------------
controller 1 APIC 1.2(3m)
.
.
.
```

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。

シスコにより、この脆弱性は Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) に影響しないことが確認されました。

侵害のインジケーター

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が新規リリースで引き続き正しくサポートされていることを十分に

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

カスタマーは、このセクションの表に沿って、適切なリリースへのアップグレードをおこなってください。 本アドバイザリは以下のアドバイザリを含むコレクションの一部です。これらも考慮した上、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。

- cisco sa-20170816 apic1： Cisco Application Policy Infrastructure Controller SSH の特権昇格の脆弱性
- cisco sa-20170816 apic2： Cisco Application Policy Infrastructure Controller カスタム バイナリの特権昇格の脆弱性

次の表では、左の列にシスコ ソフトウェアのメジャー リリースを示します。 中央の列が示すのは、本アドバイザリに記載された脆弱性によるメジャー リリースへの影響の有無、また、本脆弱性に対する修正を含む最初のマイナー リリースです。 右の列が示すのは、一連のアドバイザリに記載された脆弱性によるメジャー リリースへの影響の有無、およびそれらの脆弱性に対する最新の推奨リリースです。

Cisco Application Policy Infrastructure Controller	この脆弱性に対する最初の修正リリース	この脆弱および一連のアドバイザリに
2.0 以前	脆弱性あり; 2.2（2e）へ移行してください	2.2（2e）
2.0	脆弱性あり; 2.2（2e）へ移行してください	2.2（2e）
2.1	脆弱性あり; 2.2（2e）へ移行してください	2.2（2e）
2.2	2.2（2e）	2.2（2e）
2.3	2.3（1f）	2.3（1f）
3.0（リリース予定）	脆弱性なし	脆弱性なし

ソフトウェア更新プログラムは、cisco.com より**製品 > クラウドとシステム管理 > ポリシーとオ**

ートメーション コント ローラー > アプリケーション ポリシー インフラストラクチャ コント ローラー (APIC) と移動し、 ソフトウェア センター から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、セキュリティ研究者マネージャの Lubomir Vesely 氏により発見され、シスコに報告されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-apic2

改訂履歴

Version	Description	Section	Status	日付
1.0	Initial public release.		Final	2017-August-16

利用規約