Cisco Application Policy Infrastructure Controller Custom Binary 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 : Yes

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

ブート時間 on Cisco Application Policy Infrastructure Controller（APIC）（APIC）デバイスでインストールされたある特定の実行可能ファイル システム ファイルのためのビルド プロシージャの脆弱性はルート *レベル*特権を得る認証された、ローカル攻撃者を可能にする可能性があります。

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。 正常なエクスプロイトは攻撃者がルート *レベル*特権を得、デバイスの完全 な 制御を引き継ぐことを可能にする可能性があります。 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。

シスコはこの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ました。 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

修正済みソフトウェア

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。 修正済みソフトウェアリリースについての情報に関しては、このアドバイザリの 修正済みソフトウェアのセクションを参照して下さい。

APIC のどのリリースがデバイスで動作しているか判別するために、管理者は CLI コマンド **show version** を使用できます。 次の例はソフトウェア リリース 1.2(3m) を実行するデバイスのためのコマンドの出力を示したものです:

```
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。

改訂履歴

バージョン	説明	Section	ステータス	日付
1.0	初回公開リリース		Final	2017-August-16

利用規約