

2018年3月19日

伊藤忠テクノソリューションズ株式会社

## Cisco APIC のカスタムバイナリ特権昇格の脆弱性について

Cisco Application Policy Infrastructure Controller(APIC)にインストールされている実行可能なシステムファイルの立上げ手順に脆弱性のあることが判明しました。

この脆弱性は、ロードするライブラリを適切に検証せずに、ライブラリの相対検索パスを使用するように構築されたカスタム実行可能システムファイルに起因します。この脆弱性を利用することでローカル認証された攻撃者がルートレベルの特権を取得することが可能となります。

### ■脆弱性の詳細情報

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

### ■対象製品およびバージョン

Cisco APIC : Version 2.0 以前、2.0、2.1

### ■対処方法

恒久対策として、下記修正ソフトウェアにバージョンアップを行ってください。

使用しているソフトウェアがこの脆弱性に該当するかどうかを確認するには、下記の Cisco IOS Software Checker をご使用ください。

<https://tools.cisco.com/security/center/selectIOSVersion.x>

### ■修正ソフトウェアの入手方法

以下のサイトから入手可能です（事前にアカウント登録必要）

<http://www.cisco.com/cisco/software/navigator.html>

お問い合わせは、弊社担当営業までお願いいたします。

以上