# Cisco IOS XE ソフトウェア自律型ネットワーキング インフラストラクチャ証明書失効による脆弱性

Medium

アドバイザリーID : cisco-sa-20170726-anicrl

CVE-2017-6664

初公開日 : 2017-07-26 16:00
最終更新日 : 2018-01-31 14:47
バージョン 1.1 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCvd22328

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 IOS XEソフトウェアのAutonomic Networking(ANI)機能の脆弱性により、自律ノードの証明書が失効した後、認証されていないリモートの自律ノードが、該当システムのAutonomic Networkingインフラストラクチャにアクセスできる可能性があります。

この脆弱性は、該当ソフトウェアがAutonomic Control Plane(ACP)チャネル経由で証明書失効リスト(CRL)を転送しないことに起因しています。攻撃者は、既知の証明書および無効な証明書を持つ自律ノードを該当システムの自律ドメインに接続することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は、以前に信頼されていた自律ノードの証明書が失効した後に、該当システムの自律ドメインにそのノードを挿入できる可能性があります。

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-anicrl

## 該当製品

### 脆弱性のある製品

この脆弱性の公開時点では、Cisco IOS XEソフトウェアリリース16.xを実行し、自律型ネットワーキングを使用するように設定されているデバイスに影響が及びました。この脆弱性は、Cisco IOS XEソフトウェアの以前のリリースを実行しているデバイス、または自律型ネットワーキングを使用するように設定されていないデバイスには影響を与えません。

脆弱性が存在する Cisco IOS XE 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」セクションを参照してください。

## 自律型ネットワーキングの設定の評価

管理者は、CLIでshow running-config | include ^autonomicコマンドを使用することで、デバイスが自律型ネットワーキングを使用するように設定されているかどうかを確認できます。Cisco IOS XEソフトウェアを実行し、自律型ネットワーキングを使用するように設定されているデバイスのコマンド出力は、次の例のようになります。

```
<#root>

Router#

show running-config | include ^autonomic


autonomic
Router#
```

そのデバイスが自律型ネットワーキングを使用するように設定されていない場合、このコマンドは出力を返しません。

## Cisco IOS XE ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XE ソフトウェア リリースは、管理者がデバイスにログインして、CLI で show version コマンドを実行し、表示されるシステム バナーを参照することにより確認できます。デバイスが Cisco IOS XE ソフトウェアを実行している場合、システム バナーに「Cisco IOS Software」、「Cisco IOS XE Software」などのテキストが表示されます。

次に、Cisco IOS XR ソフトウェア リリース 16.2.1 が実行されていて、インストールされているイメージ名が CAT3K_CAA-UNIVERSALK9-M であるデバイスでのコマンドの出力例を示します。

```
<#root>

ios-xe-device#

show version
```

```
Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali 16.2.1, REL
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェアリリースの命名と番号付けの規則に関する詳細は、『White Paper: Cisco IOS and NX-OS Software Reference Guide』を参照してください。

### 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。

シスコは、この脆弱性が Cisco IOS ソフトウェア、Cisco IOS XR ソフトウェア、および Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

## 回避策

この脆弱性に対処する回避策はありません。ただし、管理者は、Autonomic Networkドメインから切断された自律ノードに対して次の操作を実行することで、この脆弱性を軽減できます。

- ノードの証明書およびキー情報が正しく削除されていることを確認します
- レジストラのAutonomic Networkingホワイトリストファイルを更新します

これらのアクションにより、自律ノードは該当システムの自律ネットワークドメインへの接続を再確立できなくなります。

## 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ソフトウェア アップデートを提供していません。

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。

## 修正済みリリース

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。お客様におかれましては、これらも考慮した上で、アップグレード ソリューション全体をご確認ください。

- cisco-sa-20170726-aniacp:Cisco IOSおよびIOS XEソフトウェア自律型コントロールプレーンチャネルにおける情報漏えいの脆弱性
- cisco-sa-20170726-anicrl:Cisco IOS XEソフトウェアAutonomic Networking Infrastructureの証明書失効の脆弱性
- cisco-sa-20170726-anidos:Cisco IOSおよびIOS XEソフトウェア自律型ネットワーキングインフラストラクチャにおけるDoS脆弱性

お客様が Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、特定のソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。 また該当する場合、そのリリースに関するすべてのアドバイザリの脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用して次のタスクを実行できます。

- ドロップダウン メニューからリリース（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- show version コマンドの出力をツールで解析する
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

公開されたシスコ セキュリティ アドバイザリのいずれかに該当するリリースであるかどうかを確認するには、Cisco.com の Cisco IOS ソフトウェアチェッカーを使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアのリリース番号（たとえば、15.1(4)M2、3.1.4S など）を入力します。

Check

## 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不正利用事例とその公表は確認しておりません。この脆弱性は、Black Hat USA 2017 カンファレンスで ERNW の Omar Eissa 氏によって発表されました。

## 出典

この脆弱性は、ERNW の Omar Eissa 氏によってシスコに報告されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-anicrl

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|
| 1.1 | Metadata update. | — | Final | 2018 年 1 月 31 日 |
| 1.0 | 初回公開リリース | — | Final | 2017 年 7 月 26 日 |

## 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。

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。