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 **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	CVE-2017-6664

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 ソフトウェアの自治ネットワーキング機能の脆弱性は自治ノードのための証明書が取り消された後非認証、リモートの、自治ノードが影響を受けたシステムの自治ネットワーキングインフラストラクチャにアクセスするようにする可能性があります。

影響を受けたソフトウェアが自治コントロール プレーン（ACP）チャネルを渡る証明書無効リスト（CRL）を転送しないので存在 する脆弱性。 攻撃者は既知のおよび取り消された証明書がある影響を受けたシステムの自治ドメインに自治ノードを接続することによってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトはノードのための証明書が取り消された後攻撃者が影響を受けたシステムの自治ドメインに以前に信頼された自治ノードを追加することを可能にす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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-anicrl

該当製品

脆弱性のある製品

パブリケーションの時に、この脆弱性は Cisco IOS XE ソフトウェアのリリース 16.x を実行して、自治ネットワーキングを使用するために設定されるデバイスに影響を与えました。 この脆弱性は自治ネットワーキングを使用するために設定されないデバイスまたはが 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に影響を与えません。

詳細についてはどのに関する Cisco IOS XE ソフトウェアがリリースするか脆弱 で、見ます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であって下さい。

自律型ネットワーキングの設定の評価

管理者は **show running-config** コマンドを使用することで、特定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判別できます。 **|** CLI の **include ^autonomic** コマンド。 次の例は Cisco IOS XE ソフトウェアを実行して、自治ネットワーキングを使用するために設定されるデバイスのためのコマンドの出力を示したものです:

```
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。

```
ios-xe-device# show version

Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali
16.2.1, RELEASE SOFTWARE (fc1)
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ついては、以下を参照してく

ださい。ホワイト ペーパー： Cisco IOS および NX-OS ソフトウェア リファレンス ガイド

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、管理者は自治ネットワーク ドメインから切断されていた自治ノードのための次の作業を行うことによってこの脆弱性を軽減できます:

- ノードのための証明書および鍵情報がきちんと削除されるようにして下さい
- レジストラの自治ネットワーキング whitelist ファイルをアップデートして下さい

これらの操作は自治ノードが影響を受けたシステムの自治ネットワーク ドメインに接続を再確立することを防ぎます。

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

- 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 Denial Of Service（DoS）の脆弱性

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できるよう、シスコでは Cisco IOS Software Checker ツールを提供しています。このツールにより、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、すべてのアドバイザリに記載されたすべて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含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全アドバイザリを含めるなど）を作成する

リリースが、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かどうかを確認するには、Cisco.com の Cisco IOS Software Checker 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 リリース（たとえば、**15.1(4)M2**、**3.1.4S** など）を入力します。

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は確認していません。 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-anicrl

改訂履歴

Version	Description	Section	Status	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-July-26

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。