Cisco IOS XR for NCS 6000のパケットタイマーリークによるDoS脆弱性

High

アドバイザリーID : cisco-sa-20160713-ncs6k
初公開日 : 2016-07-13 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 : CSCux76819

CVE-2016-1426

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 Network Convergence System 6000(NCS 6000)シリーズルータ向けCisco IOS XRのシステムタイマーリソースの管理における脆弱性により、認証されていないリモートの攻撃者がシステムタイマーリソースのリークを引き起こし、非動作状態になり、最終的に該当プラットフォームでルートプロセッサ(RP)のリロードが発生する可能性があります。

この脆弱性は、システムタイマーリソースの不適切な管理に起因します。攻撃者は、多数のSecure Shell(SSH)、Secure Copy Protocol(SCP)、およびSecure FTP(SFTP)管理接続を該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はシステムタイマーリソースのリークを引き起こし、非稼働状態になり、最終的に該当プラットフォームでRPのリロードが発生する可能性があります。
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ています。この脆弱性を軽減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で確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160713-ncs6k

該当製品

脆弱性のある製品

該当バージョンのCisco IOS XRが稼働しているCisco NCS 6000には、デバイスへのSSH、SCP、およびSFTP管理接続を処理するように設定されている場合に脆弱性が存在します。脆

弱性が存在するCisco NCS 6000用Cisco IOS XR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。

この脆弱性は、IPv4 パケットまたは IPv6 パケットのどちらでも不正利用される可能性があります。この脆弱性は、TCPリスニングポート22またはこれらのサービス用に設定されたその他のTCPポートを宛先とするSSH、SCP、またはSFTP管理接続によって引き起こされる可能性があります。また、デバイスに設定された任意のインターフェイスのIPv4またはIPv6ユニキャストアドレスを使用する可能性もあります。攻撃者はTCP 3ウェイハンドシェイクを確立する必要がありますが、脆弱なデバイスへの管理接続を認証する必要はありません。

この脆弱性は、該当デバイスを宛先とするトラフィックによってのみトリガーされ、該当デバイスを通過するトラフィックを使用して不正利用されることはありません。

SSH、SCP、またはSFTPが管理アクセス用に設定されているかどうかを確認するには、 **show running-config | include ssh server**コマンドを使用して、 **ssh server v2**コマンドが存在することを確認します。

次の例は、SSHv2サーバが有効になっているCisco IOS XRルータを示しています。

```
RP/0/RP0/CPU0:router#sho run | in ssh server
Thu Jun 16 06:44:34.256 CEST
Building configuration...
ssh server v2 ssh server vrf default
```

Cisco IOS XR ソフトウェア リリースの判別

デバイスで実行されているCisco IOS XRソフトウェアリリースと、そのリリースが実行されているデバイスの名前を確認するには、管理者がデバイスにログインして、コマンドラインインターフェイス(CLI)で **show version**コマンドを使用します。デバイスが Cisco IOS XR 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 XR Software 」などのテキストが表示されます。ハードウェア製品の名前はシステム イメージ ファイル ロケーションの次の行に表示されます。

以下は、Cisco IOS XR ソフトウェア リリース 5.2.5 が稼働中のデバイスで **show version command コマンドを実行した場合の出力例です。**

```
RP/0/RP0/CPU0:ios#show version
Wed Jun 15 16:08:37.966 UTC

Cisco IOS XR Software, Version 5.2.5
Copyright (c) 2013-2014 by Cisco Systems, Inc.

Build Information:
```

```
 Built By     : ahoang
 Built On     : Thu Mar 17 19:26:37 PDT 2016
 Build Host   : iox-lnx-006
 Workspace    : /auto/srcarchive16/production/5.2.5/all/workspace
 Version      : 5.2.5
 Location     : /opt/cisco/XR/packages/

cisco NCS-6000 () processor
System uptime is 6 weeks, 6 days, 19 hours, 32 minutes
```

脆弱性を含んでいないことが確認された製品

Cisco IOS XRを実行しているCisco 12000シリーズルータ、Cisco ASR 9000シリーズアグリゲーションサービスルータ、Cisco Carrier Routing System、およびCisco Network Convergence System 4000シリーズは、この脆弱性の影響を受けません。

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。

セキュリティ侵害の痕跡

この脆弱性が不正利用されるデバイスでは、ルートプロセッサ(RP)が新しいプロセスを作成できず、フリーズし、ルーティングプロトコルパケットと管理接続のドロップを開始する可能性があり、最終的にリロードが発生します。デバイス宛てのすべてのトラフィックと、ルーティングプロトコルから学習した情報に依存するパススルートラフィックは、リロードプロセス中にドロップされ、サービス拒否(DoS)状態を引き起こします。

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リリースしています。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、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。

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場合は、http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、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 Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。

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

この脆弱性は、Cisco IOS XRソフトウェアの次のソフトウェアメンテナンスアップデート(SMU)で修正されています。

- ncs6k-5.2.5.CSCux76819.smu
- ncs6k-5.2.4.CSCux76819.smu
- ncs6k-5.2.3.CSCux76819.smu
- ncs6k-5.2.1.CSCux76819.smu
- ncs6k-5.0.1.CSCux76819.smu

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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やその公表を確認していません。

出典

この脆弱性はサポート ケースの解決中に発見されました。

URL

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

20160713-ncs6k

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	-	Final	2016年7月13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。