Cisco IOS および IOS XE ソフトウェアでの巧妙に細工された Network Time Protocol パケットによる Denial Of Service（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20160804-wedge

初公開日 : 2016-08-04 16:00

最終更新日 : 2018-02-27 12:37

バージョン 1.3 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCva35619

CVE-2016-1478

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 および Cisco IOS XE による Network Time Protocol（NTP）パケットの処理に関する脆弱性により、認証されていないリモート攻撃者が該当デバイスにインターフェイス ウェッジを発生させ、最終的に Denial Of Service（DoS）状態を引き起こす可能性があります。

この脆弱性の原因は、インターフェイス キューから送信された無効な NTP パケットをクリアできているかどうかのチェックが不十分なことにあります。 攻撃者は、NTP パケットを処理するように設定された該当デバイスに、巧妙に細工された NTP パケットを大量に送信することにより、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、攻撃者は該当デバイスにインターフェイス ウェッジを発生させ、最終的に Denial Of Service（DoS）状態を引き起こす可能性があります。

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ました。 この脆弱性に対処する回避策はありませんが、 ただし、この脆弱性に対しては回避策があります。

このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160804-wedge

該当製品

脆弱性のある製品

次の Cisco IOS ソフトウェア リリース、および対応する IOS XE ソフトウェア リリースはこの脆弱性の影響を受けます。

- 15.5(3)S3 - 3.16.3S
- 15.6(1)S2 - 3.17.2S
- 15.6(2)S1 - 3.18.1S
- 15.6(2)T1

影響を受ける IOS または IOS XE ソフトウェアのバージョンを実行しているシスコ デバイスは、NTP オペレーション用に設定されている場合に脆弱です。 NTP は、Cisco IOS または IOS XE ソフトウェアではデフォルトで無効になっています。

デバイスが NTP 用に設定されているかどうかを確認するには、デバイスにログインして、次の CLI コマンドを発行します： **show running-config | include ntp**。 出力に次のいずれかのコマンドが返された場合、そのデバイスは脆弱です。

```
ntp master <any following commands>
ntp peer <any following commands>
ntp server <any following commands>
ntp broadcast client
ntp multicast client
```

次の例は、NTP 用に設定されているシスコ デバイスを示しています。

```
router#show running-config | include ntp
ntp peer 192.168.0.12
```

次の例は、NTP 用に設定されていないシスコ デバイスを示しています。

```
router#show running-config | include ntp
router#
```

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、デバイスに構成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、あるいはネットワーク アドレスを使用して、UDP リスニング ポート 123 を宛先とする巧妙に細工された NTP パケットを送信することでトリガーされます。

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。

Cisco IOS または IOS XE ソフトウェア リリースの判別

Cisco IOS 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 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、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、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 ソフトウェアを実行している場合、システム バナーに「*Cisco Internetwork Operating System Software*」や「*Cisco IOS Software*」などのテキストが表示されます。 バナーにはインストールされたイメージ名もカッコ内に表示され、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリ

ース名が表示されます。 一部のシスコ デバイスでは、**show version** コマンドをサポートしていなかったり、別の出力が表示されたりします。

次の例は、Cisco IOS ソフトウェア リリースが 15.5(2)T1 で、インストールされたイメージ名が *C2951-UNIVERSALK9-M* であるシスコ製品を示しています。

```
Router> show version
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
.
.
.
```

Cisco IOS 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。

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、巧妙に細工された NTP パケットは受信インターフェイスの入力キューでスタックし、結果的にそのキューがウェッジされます。 インターフェイスがウェッジされると、ルータがリロードされるまでトラフィックの受信が停止します。

回避策

この脆弱性に対処する回避策はありませんが、 ただし、この脆弱性に対しては回避策があります。

回避策として、インターフェイス アクセス リスト（ACL）を使用してコントロール プレーン ポリシング（CoPP）を実行し、既知の NTP ピアから受信する NTP トラフィックを制限します。 このような緩和策を導入することによって有効な NTP トラフィックが破棄されないようにするためには、ネットワーク管理者が詳細な専門知識を駆使して慎重に設定する必要があります。 この脆弱性の対象となっている NTP プロトコルは伝送手段として UDP を使用するため、送信者の IP アドレスをスプーフィングすることにより、信頼できる IP アドレスからそれらのポートへの通信を許可する ACL を無効化することができます。

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無償のソフトウェア アップデートを提

供しています。 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。

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、次の Cisco IOS ソフトウェアおよび対応する Cisco IOS XE ソフトウェア リリースで修正されています。

- 15.6(3)M
- 15.6(2)SP - 3.18.0SP

シスコは、利用可能になり次第、残りの該当リリースに対する修正済みソフトウェアをリリースします。

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

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160804-wedge

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.3	回避策セクションを更新。すべてのインターフェイス タイプを網羅するために、コントロール プレーン ポリシング（CoPP）の使用を記載。	回避策	最終版	2018 年 2 月 27 日
1.2			最終版	2016 年 10 月 6 日
1.1	対応する該当 IOS XE ソフトウェア リリースを特定。	脆弱性のある製品	最終版	2016 年 8 月 9 日
1.0	初回公開リリース	â	最終版	2016 年 8 月 4 日

利用規約