Cisco IOSソフトウェア Network Time Protocol（NTP）パケットの脆弱性

High

アドバイザリーID : cisco-sa-20090923-ntp

初公開日 : 2009-09-23 16:00

バージョン 1.1 : Final

CVSSスコア : 7.8

回避策 : No Workarounds available

Cisco バグ ID : CSCsu24505 CSCsv75948

CVE-2009-2869

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

ネットワーク タイム プロトコル（NTP）バージョン（v4）のためのサポートの Cisco IOSÂ® ソフトウェアはデバイスのリロードという結果に終る特定の NTP パケットを処理する脆弱性が含まれています。 これは影響を受けたデバイスのリモート サービス拒否 （DoS）状態という結果に終ります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。

この脆弱性を軽減する回避策は利用できます。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-ntp で掲示されます。

注: 2009 年 9 月 23 日の IOS アドバイザリ バンドル公開には 11 件の Security Advisory が含まれています。 10 件のアドバイザリは Cisco IOS ソフトウェアの脆弱性に対処するもので、 1 件は Cisco Unified Communications Manager の脆弱性に対処するものです。 各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決するリリースを記載しています。

"Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" の個々の公開リンクは次のリンク内に掲載されています:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

該当製品

脆弱性のある製品

Cisco IOSソフトウェア デバイスは NTPv4 をサポートすればで、NTP オペレーションのために設定されます脆弱。 NTP は Cisco IOSソフトウェアでデフォルトで有効に なりません。

デバイスサポート NTPv4 が Command Line Interface （CLI）のコンフィギュレーションモードによって、デバイスにログイン するかどうか見ることは、コマンド **NTP ピア 127.0.0.1 バージョンを**入力し、**か**。 出力にオプションとして第 **4 が**ある場合、そしてデバイスサポート NTPv4。 次の例は NTPv4 をサポートする Cisco IOS ソフトウェア リリースを実行しているCiscoデバイスを識別したものです:

```
Router#configure terminal
Router(config)#ntp peer 127.0.0.1 version ?
  <2-4>  NTP version number
```

次の例は NTPv4 をサポートしない Cisco IOS ソフトウェア リリースを実行している Ciscoデバイスを識別したものです:

```
Router(config)#ntp peer 127.0.0.1 version ?
  <1-3>  NTP version number
```

デバイスが NTP で設定されるかどうか見るために、デバイスにログイン し、CLI コマンド **show running-config を**発行して下さい **| NTP を含んで下さい**。 出力が戻れば次のコマンドのどちらかはそれからデバイスをです脆弱リストしました:

```
Router(config)#ntp peer 127.0.0.1 version ?
  <1-3>  NTP version number
```

次の例は NTP で設定される Ciscoデバイスを識別したものです:

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

次の例は NTP で設定されない Ciscoデバイスを識別したものです:

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

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他のシスコ デバイスでは、**show version** コマンドが存在しなかったり、別の出力が表示されたりします。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
Router#show version
 Cisco Internetwork Operating System Software
 IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
 Technical Support: http://www.cisco.com/techsupport
 Copyright Â©) 1986-2008 by cisco Systems, Inc.
 Compiled Mon 17-Mar-08 14:39 by dchih

 <output truncated>
```

以下の例は、Cisco 製品にて、IOSリリース 12.4(20)T が稼動し、そのイメージ名が C1841-ADVENTERPRISEK9-M であることを示しています:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright Â©) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide" で確認できます: http://www.cisco.com/warp/public/620/1.html。

脆弱性を含んでいないことが確認された製品

以下の製品または機能はこの脆弱性の影響を受けません:

- NTPv4 のためのサポートのない Cisco IOSソフトウェア デバイス
- 簡単な NTP （ SNTP ）機能だけで設定される Cisco IOSソフトウェア デバイス
- Cisco IOS XE ソフトウェア
- Cisco IOS XR ソフトウェア

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。

詳細

ネットワーク タイム プロトコル (NTP) はマシンのネットワークの時刻を同期化するように設計されているプロトコルです。 NTP はそれから IP を実行する UDP を実行します。 NTPv3 は RFC1305 で文書化されています 。 NTPv4 は NTP 規格の重要な修正でが、現在の開発バージョンで、RFC にこのアドバイザリのパブリケーションの時に形式化されませんでした。 NTPv4 は draft-ietf-ntp-ntpv4-proto-11 で現在 文書化されています

NTPv4 をサポートする Cisco IOSソフトウェア デバイスは仕様 NTP パケットを受信する場合 NTP リプライパケットを作成している間クラッシュします。 NTP パケットはあらゆるリモートデバイスから送信 することができ認証を必要としません。 NTPv4 をサポートし、NTP ピア 認証

で設定される Cisco IOSデバイスはまだ脆弱です。 デバイスは NTPv4 同位のために明示的に設定される必要がありません。 バージョン 2 で明示的に分類されるすべての NTP 同位で設定されたたとえばデバイスはまだ次の例に示すように脆弱、です:

```
Router#show running-config | include ntp
ntp peer 192.168.0.254 version 2
ntp peer 192.168.0.1 version 2
Router#
```

NTP の Ciscoインプリメンテーションのさらに詳しい詳細については、コンフィギュレーションガイド「Cisco IOS および NX-OS ソフトウェア参照しま-基本システム管理」を次のリンクで行います:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1001170

この脆弱性は次の Cisco バグ ID で文書化されています: CSCsu24505 （登録ユーザのみ）および CSCsv75948 （登録ユーザのみ）はおよびよくある脆弱性および公開（CVE）識別子 CVE-2009-2869 は割り当てられました。 この脆弱性への完全な解決法に Cisco バグ ID が両方とも必要となります。

回避策

回避策はデバイスの NTP をディセーブルにすること以外ありません。 次の軽減はこの脆弱性のために識別されました; デバイスのあらゆる構成されたIPアドレスに宛てたパケットだけこの脆弱性を不正利用できます。 トランジットトラフィックはこの脆弱性を不正利用しません。

注: NTP ピア 認証は回避策でし、今でも脆弱 な 設定です。

NTP アクセスグループ

警告： この脆弱性の機能は転送するとして UDP を利用するので、信頼された IP アドレスからのこれらのポートにアクセス コントロール リスト（ACL）をその割り当て通信敗北させるかもしれない送信側の IP アドレスをスプーフィングすることは可能性のあるです。 Unicast Reverse Path Forwarding（uRPF）（ユニキャスト RPF）結合でよりよい軽減ソリューションを提供するのに使用されると考慮されるべきです。

```
Router#show running-config | include ntp
ntp peer 192.168.0.254 version 2
ntp peer 192.168.0.1 version 2
Router#
```

警告： NTP ACL構成によっては、Cisco バグ ID を理解しておいて下さい: CSCsw79186 （登録ユーザのみ） - NTPv4 サーバは「ピア」として NTPv3 クライアントを扱います。

NTP アクセスコントロール グループのその他の情報に関しては、次のリンクで「タイトルを付けられる文書を参照しま基本システム管理」を行います:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

インフラストラクチャ アクセス コントロール リスト

警告： この脆弱性の対象となっている機能は伝送手段として UDP を用いているため、送信元 IP アドレスを詐称し、これらのUDPポート宛の、信用された送信元 IP アドレスのみを許可するような ACL では防ぎきれない場合もあります。 より有効な緩和策としてユニキャスト RPF を併用することもお勧めします。

ネットワークを通過するトラフィックを遮断することはしばしば困難ですが、インフラストラクチャ デバイスをターゲットとした許可すべきではないトラフィックを特定し、そのようなトラフィックをネットワークの境界で遮断することは可能です。 インフラストラクチャ ACL（iACLs）はネットワーク セキュリティ 最良 の 方法で、よいネットワーク セキュリティへの長期付加、またこの特定の脆弱性のための回避策として考慮する必要があります。 iACL 下記の例はインフラストラクチャ IPアドレス範囲の IP アドレスのすべてのデバイスの保護を助ける展開されたインフラストラクチャ access-list の一部として含まれるはずです:

```
Router#show running-config | include ntp
ntp peer 192.168.0.254 version 2
ntp peer 192.168.0.1 version 2
Router#
```

ホワイトペーパー 『Protecting Your Core: インフラストラクチャ 保護はアクセス コントロール リスト（ACL）」インフラストラクチャ 保護 アクセス リストのためのガイドラインおよび推奨される配備手法を示し、次のリンク http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml で利用できます

コントロール プレーン ポリシング

警告： この脆弱性の対象となっている機能は伝送手段として UDP を用いているため、送信元 IP アドレスを詐称し、これらのUDPポート宛の、信用された送信元 IP アドレスのみを許可するような ACL では防ぎきれない場合もあります。 より有効な緩和策としてユニキャスト RPF を併用することもお勧めします。

コントロール プレーン ポリシング（CoPP）がデバイスに信頼できない UDP トラフィックをブロックするのに使用することができます。 Cisco IOS ソフトウェア リリース 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T は、CoPP 機能をサポートしています。 CoPP はデバイスで管理および制御平面を保護し、既存 の セキュリティポリシーおよびコンフィギュレーションに従ってインフラストラクチャ デバイスに送信 される 明示的に承認されたトラフィックだけ許可することによって直接インフラストラクチャ不正侵入のリスクおよび効果を最小に するのを助けるために設定することができます。 CoPP 下記の例はインフラストラクチャ IPアドレス範囲の IP アドレスのすべてのデバイスの保護を助ける展開された CoPP の一部として含まれるはずです。

```
Router#show running-config | include ntp
ntp peer 192.168.0.254 version 2
ntp peer 192.168.0.1 version 2
Router#
```

上記の CoPP の例では、"permit" アクションであるアクセスコントロールリストエントリ (ACE) に該当し、攻撃である可能性のあるパケットは、policy-map の "drop" 機能により廃棄されますが、一方、"deny" アクション(記載されていません)に該当するパケットは、policy-map の "drop" 機能の影響を受けません。 以下の事項に注意して下さい: policy-map 構文は 12.2S および 12.0S 一連のCisco IOSソフトウェアで異なっています:

```
Router#show running-config | include ntp
ntp peer 192.168.0.254 version 2
ntp peer 192.168.0.1 version 2
Router#
```

CoPP 機能の設定および使用のその他の情報は次のリンクで文書で、「コントロール プレーン ポリシング 実装 最良 の 方法」および「Cisco IOS ソフトウェア リリース 12.2 S -コントロール プレーン ポリシング」見つけることができます:
http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html および
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

いずれの場合も、アップグレードする機器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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。 情報に不明な点がある場合は、Cisco Technical Assistance Center (TAC) または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表 (下掲) の各行には、Cisco IOS のリリース トレインが記載されています。 特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース (および、それぞれの予想提供日) が表の「第 1 修正済みリリース」列に記載されます。 「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。 特定の列に記されているリリースよりも古い (第 1 修正済みリリースより古い) トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。 表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャー リリース	修正済みリリースの入手可能性	
Affecte	First Fixed Release (修正された最	推奨リリ

d 12.0-Based Releases	**初のリリース）**	**ース**
該当する 12.0 ベースのリリースはありません。		
Affected 12.1-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.1 ベースのリリースはありません。		
Affected 12.2-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.2 基づいたリリースがありません		
Affected 12.3-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.3 ベースのリリースはありません。		
Affected 12.4-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
12.4	脆弱性なし	
12.4GC	脆弱性なし	
12.4JA	脆弱性なし	
12.4JDA	脆弱性なし	
12.4JDC	脆弱性なし	
12.4JDD	脆弱性なし	
12.4JK	脆弱性なし	
12.4JL	脆弱性なし	
12.4JMA	脆弱性なし	
12.4JMB	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	12.4(22)MD 以前のリリースは 12.4(22)MD で脆弱、脆弱性最初に導入されました、first fixed in 12.4(22)MD1 ではないです。	12.4(22)MD1

12.4MDA	脆弱性なし	
12.4MR	脆弱性なし	
12.4SW	脆弱性なし	
12.4T	12.4(20)T 以前のリリースは脆弱ではないです。 12.4(20)T および 12.4(20)T1 は脆弱、脆弱性です first fixed in 12.4(20)T2 です。 12.4(22)T は脆弱、脆弱性です first fixed in 12.4(22)T1 です 12.4(24)T は脆弱ではないです。	12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XA	脆弱性なし	
12.4XB	脆弱性なし	
12.4XC	脆弱性なし	
12.4XD	脆弱性なし	
12.4XE	脆弱性なし	
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	
12.4XJ	脆弱性なし	
12.4XK	脆弱性なし	
12.4XL	脆弱性なし	
12.4XM	脆弱性なし	
12.4XN	脆弱性なし	
12.4XP	脆弱性なし	
12.4XQ	脆弱性なし	
12.4XR	脆弱性なし	
12.4XT	脆弱性なし	
12.4XV	脆弱性なし	
12.4XW	脆弱性なし	
12.4XY	脆弱性なし	
12.4XZ	脆弱性あり; first fixed in 12.4T	12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4YA	脆弱性あり; first fixed in 12.4T	12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-

		OCT-2009 で利用可能
12.4YB	脆弱性なし	
12.4YD	12.4(22)YD1	12.4(22)YD1
12.4YE	12.4(22)YE1	12.4(22)YE1

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の公示か不正利用に気づいていません。

この脆弱性は Cisco によってカスタマー サポートを処理するとき呼出します検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-ntp

改訂履歴

リビジョン 1.0	2009-September-23	初版リリース

利用規約