Cisco IOS Software Multicast Network Time Protocol Denial of Service Vulnerability

Advisory ID: cisco-sa-20130925-ntp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ntp

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。

Revision 1.0

For Public Release 2013 September 25 16:00 UTC (GMT)

目次

要約

Cisco IOS ソフトウェアのネットワーク タイム プロトコル（NTP）機能の実装面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によって該当デバイスがリロードさせられる可能性があり、その結果、サービス拒否（DoS）が発生することがあります。

この脆弱性は、MSDP ピアから、Multicast Source Discovery Protocol（MSDP）Source-Active（SA）メッセージでカプセル化された該当デバイス宛てへのマルチキャスト NTP パケットの処理が不適切なことに起因します。攻撃者は、マルチキャスト NTP パケット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できます。不正利用が繰り返されると、DoS 状態が続く可能性があります。

シスコはこの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ました。この脆弱性には回避策があります。

このアドバイザリは、次のリンク先で入手できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ntp

注：2013 年 9 月 25 日の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開には、8 件のセキュリティ アドバイザリが含まれています。これらのアドバイザリはすべて、Cisco IOS ソフトウェアの脆弱性に対処するものです。各 Cisco IOS ソフトウェア セキュリティ 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修正する Cisco IOS ソフトウェア リリース、および 2013 年 9 月にバンドル公開したすべての Cisco IOS ソフトウェアの脆弱性を修正する Cisco IOS ソフトウェア リリースを記載しています。

個別の公開リンクは、次のリンクにある「Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

該当製品

脆弱性が認められる製品

Cisco IOS ソフトウェア リリースが稼働しているシスコ デバイスが、次の 2 つの条件を満たしている場合、脆弱性に該当します。

- デバイス構成に、マルチキャスト NTP コンフィギュレーション コマンドが含まれている
- デバイスに最低 1 つの MSDP ピアが設定されている

show running-config | include ^interface|ntp multicast 特権 EXEC コマンド：デバイス構成にマルチキャスト NTP コンフィギュレーション コマンドが含まれているかどうかの判別に使用できます。Cisco IOS ソフトウェアが稼働していて、複数のインターフェイスにマルチキャスト NTP が設定されているデバイスに **show running-config | include ^interface|ntp multicast** コマンドを実行すると、次のような出力が表示されます。

```
Router#show running-config | include ^interface|ntp multicast
interface Loopback0
interface Loopback1
interface FastEthernet0/0
ntp multicast
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet1/0
ntp multicast key 61560
interface FastEthernet1/1
interface FastEthernet1/2
ntp multicast client
interface FastEthernet1/3
ntp multicast client
ntp multicast
Router#
```

注：デバイス構成にマルチキャスト NTP コマンドが含まれていない場合は、次の手順は省略できます。そのデバイスに脆弱性はありません。

show ip msdp summary 特権 EXEC コマンド：デバイスに最低 1 つの MSDP ピアが設定されているかどうかを判別するのに使用できます。下記は、1 つの MSDP ピアが設定されている Cisco IOS ソフトウェアが稼働するデバイス上で実行された **show ip msdp summary** コマンドからの出力です。

```
Router#show ip msdp summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
10.54.54.54      ?     Up       00:35:03 0     6     ?
Router#
```

MSDP ピアが設定されていないデバイスには、脆弱性はありません。

NTP マルチキャスト パケットの処理は、デフォルトでは有効になっていません。

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインし **show version** コマンドを実行してシステム バナーを表示させます。「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、続いてバージョンと Cisco IOS ソフトウェア 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** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で Cisco IOS ソフトウェア リリース 15.0(1)M1 が稼働し、インストールされているイメージ名が C3900-UNIVERSALK9-M であることを示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_teamRouter> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
```

Cisco IOS ソフトウェアのリリース命名規則の追加情報は以下のリンクにある「White Paper: Cisco IOS and NX-OS Software Reference Guide」で確認できます。
http://www.cisco.com/web/about/security/intelligence/ios-ref.html

脆弱性が認められない製品

次の製品はこの脆弱性の影響を受けないことが確認されています。

- Cisco IOS XR Software

この脆弱性の影響を受ける他のシスコ製品は、現在確認されていません。

詳細

NTP は、ネットワーク上のマシン間の時刻の同期化を目的に設計されています。NTP は UDP 上で動作し、IP で転送されます。NTP を実行しているネットワーキング デバイスは、時刻を基準時刻源と同期する際にさまざまなアソシエーション モードで動作するように設定できます。ネットワーキング デバイスは、2 つの方法でネットワーク上の時刻情報を取得できます。2 つの方法とは、ホスト サーバーへのポーリングと NTP ブロードキャストのリスニングです。

Cisco IOS ソフトウェアのネットワーク タイム プロトコル（NTP）機能の実装面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によって該当デバイスがリロードさせられる可能性

があり、その結果、サービス拒否（DoS）が発生することがあります。

この脆弱性は、設定されている MSDP ピアから、Multicast Source Discovery Protocol（MSDP）Source-Active（SA）メッセージでカプセル化された該当デバイス宛てへのマルチキャスト NTP パケットの処理が不適切なことに起因します。攻撃者は、マルチキャスト NTP パケット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できます。不正利用が繰り返されると、DoS 状態が続く可能性があります。

この脆弱性は、Cisco Bug ID CSCuc81226（ 登録ユーザ専用 ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2013-5472 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCuc81226:Cisco IOS Software Multicast NTP Denial of Service Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.1**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Complete
CVSS Temporal Score - **5.9**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性が悪用されると、該当するデバイスが再起動する可能性があります。不正利用が繰り返されると、DoS 状態が続く可能性があります。

ソフトウェア バージョンおよび修正

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, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

Cisco IOS ソフトウェア

Cisco IOS ソフトウェア テーブル（下記）の各行は Cisco IOS ソフトウェア トレインを示します。あるトレインが脆弱性を含む場合、修正を含む最初のリリースは「First Fixed Release」列に示されます。「First Fixed Release for All Advisories in the September 2013 Bundled Publication」列は、その Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開で公開済みであるすべての脆弱性を修正する最初のリリースを示します。可能な限り、最新のリリースにアップグレードすることを推奨します。

Cisco IOS ソフトウェア チェッカーを利用して、特定の Cisco IOS ソフトウェア リリースに対応したシスコのセキュリティ アドバイザリを検索することができます。このツールは次の Cisco Security Intelligence Operations（SIO）ポータルで利用できます。
http://tools.cisco.com/security/center/selectIOSVersion.x

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2013 Bundled Publication
12.0S	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.0SY	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.0SZ	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
Affected 12.2-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2013 Bundled Publication
12.2EX	Note: Releases prior to 12.2(58)EX are vulnerable; Releases 12.2(58)EX and later are not vulnerable.	Vulnerable; First fixed in Release 15.0SE

12.2EY	Note: Releases prior to 12.2(58)EY are vulnerable; Releases 12.2(58)EY and later are not vulnerable.	Vulnerable; First fixed in Release 15.2S
12.2EZ	Note: Releases prior to 12.2(58)EZ are vulnerable; Releases 12.2(58)EZ and later are not vulnerable.	Releases prior to 12.2(60)EZ2 are vulnerable; Releases 12.2(60)EZ2 and later are not vulnerable.First fixed in Release 15.0SE
12.2IRB	Vulnerable; First fixed in Release 12.2SRE	Vulnerable; First fixed in Release 12.2SRE
12.2IRC	Vulnerable; First fixed in Release 12.2SRE	Vulnerable; First fixed in Release 12.2SRE
12.2IRD	Vulnerable; First fixed in Release 12.2SRE	Vulnerable; First fixed in Release 12.2SRE
12.2IRE	Vulnerable; First fixed in Release 12.2SRE	Vulnerable; First fixed in Release 12.2SRE
12.2IRF	Vulnerable; First fixed in Release 12.2SRE	Vulnerable; First fixed in Release 12.2SRE
12.2IRG	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IRH	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IRI	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXG	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXH	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2MC	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.2MRA	Vulnerable; First fixed in Release 12.2SRE	Vulnerable; First fixed in Release 12.2SRE
12.2MRB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SB	12.2(33)SB15	12.2(33)SB15
12.2SCA	Vulnerable; First fixed in Release 12.2SCH	Vulnerable; First fixed in Release 12.2SCH
12.2SCB	Vulnerable; First fixed in Release 12.2SCH	Vulnerable; First fixed in Release 12.2SCH
12.2SCC	Vulnerable; First fixed in Release 12.2SCH	Vulnerable; First fixed in Release 12.2SCH
12.2SCD	Vulnerable; First fixed in Release 12.2SCH	Vulnerable; First fixed in Release 12.2SCH
12.2SCE	Vulnerable; First fixed in Release 12.2SCH	Vulnerable; First fixed in Release

		12.2SCH
12.2SCF	Vulnerable; First fixed in Release 12.2SCH	Vulnerable; First fixed in Release 12.2SCH
12.2SCG	Vulnerable; First fixed in Release 12.2SCH	Vulnerable; First fixed in Release 12.2SCH
12.2SCH	12.2(33)SCH1	12.2(33)SCH1
12.2SE	12.2(55)SE8 12.2(58)SE	12.2(55)SE8
12.2SEG	Vulnerable; migrate to any release in 15.0SE	Vulnerable; First fixed in Release 15.0SE
12.2SG	12.2(53)SG10; available December 2013 *	12.2(53)SG10; available December 2013 *
12.2SGA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SM	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SQ	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SRA	Vulnerable; First fixed in Release 12.2SRE	Vulnerable; First fixed in Release 12.2SRE
12.2SRB	Vulnerable; First fixed in Release 12.2SRE	Vulnerable; First fixed in Release 12.2SRE
12.2SRC	Vulnerable; First fixed in Release 12.2SRE	Vulnerable; First fixed in Release 12.2SRE
12.2SRD	Vulnerable; First fixed in Release 12.2SRE	Vulnerable; First fixed in Release 12.2SRE
12.2SRE	12.2(33)SRE9	12.2(33)SRE9
12.2STE	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SV	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SVD	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SVE	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SW	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.2SXF	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this

		advisory.
12.2SXH	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXI	12.2(33)SXI12	12.2(33)SXI12
12.2SXJ	Not vulnerable	12.2(33)SXJ6
12.2SY	Vulnerable; First fixed in Release 15.0SY	Vulnerable; First fixed in Release 15.0SY
12.2WO	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2XNA	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNB	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNC	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XND	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNE	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNF	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XO	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZYA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Bundled Publication**
12.3BC	Vulnerable; First fixed in Release 12.2SCH	Vulnerable; First fixed in Release 12.2SCH
12.3JEC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JED	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JEE	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.3JX	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.3XI	Vulnerable; First fixed in Release 12.2SB	Vulnerable; First fixed in Release 12.2SB
12.3XJ	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3XK	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3XL	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3XQ	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3XR	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M

12.3XU	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3XW	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3XX	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YD	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YF	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YG	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YI	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YJ	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YK	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YM	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YQ	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YS	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YT	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YU	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YX	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.3YZ	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3ZA	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
Affected 12.4-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Bundled Publication**
12.4	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4GC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JA	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.4JAL	Not vulnerable	Vulnerable; First fixed in Release 12.4JAM
12.4JAM	Not vulnerable	12.4(25e)JAM2
12.4JAN	Not vulnerable	Not vulnerable
12.4JAX	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.4JAZ	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JDA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JDC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JDD	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JDE	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.4JHA	Not vulnerable	Vulnerable; contact your support organization per the instructions in

		Obtaining Fixed Software section of this advisory.
12.4JHB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JHC	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.4JK	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JL	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JX	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.4JY	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.4JZ	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.4MD	Note: Releases prior to 12.4(22)MD are vulnerable; Releases 12.4(22)MD and later are not vulnerable.	Vulnerable; First fixed in Release 12.4MDB
12.4MDA	Not vulnerable	Vulnerable; First fixed in Release 12.4MDB
12.4MDB	Not vulnerable	12.4(24)MDB15
12.4MR	Note: Releases prior to 12.4(20)MR are vulnerable; Releases 12.4(20)MR and later are not vulnerable.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4MRA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4MRB	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.4SW	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4T	Note: Releases prior to 12.4(20)T are vulnerable; Releases 12.4(20)T and later are not vulnerable.	Vulnerable; First fixed in Release 15.1M
12.4XA	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XB	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XC	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XD	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XE	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XF	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XG	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XJ	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XK	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XL	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XM	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XN	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this

		advisory.
12.4XP	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XQ	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XR	Note: Releases prior to 12.4(22)XR are vulnerable; Releases 12.4(22)XR and later are not vulnerable.	Vulnerable; First fixed in Release 15.1M
12.4XT	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XV	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XW	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XY	Vulnerable; migrate to any release in 15.0M	Vulnerable; First fixed in Release 15.1M
12.4XZ	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.4YA	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.4YB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4YD	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4YE	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.4YG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
Affected 15.0-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Bundled Publication**
15.0EA	Not vulnerable	15.0(2)EA1
15.0EB	Not vulnerable	Vulnerable; migrate to any release in 15.2E
15.0EC	Not vulnerable	Vulnerable; migrate to any release in 15.2E
15.0ED	Not vulnerable	Note: Releases prior to 15.0(2)ED1 are vulnerable; Releases 15.0(2)ED1 and later are not vulnerable.
15.0EH	Not vulnerable	Not vulnerable
15.0EJ	Not vulnerable	Not vulnerable
15.0EX	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0EY	Not vulnerable	15.0(2)EY2
15.0EZ	Not vulnerable	Only Release 15.0(2)EZ is vulnerable
15.0M	Not vulnerable	Vulnerable; First fixed in Release 15.1M
15.0MR	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this

		advisory.
15.0S	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Vulnerable; First fixed in Release 15.1S Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SE	Not vulnerable	15.0(2)SE4
15.0SG	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SQA	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SQB	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SY	15.0(1)SY3	15.0(1)SY5
15.0XA	Not vulnerable	Vulnerable; First fixed in Release 15.1M
15.0XO	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
Affected 15.1-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Bundled Publication**
15.1EY	Not vulnerable	Vulnerable; First fixed in Release 15.2S
15.1GC	Not vulnerable	Vulnerable; First fixed in Release 15.1M
15.1M	Not vulnerable	15.1(4)M7
15.1MR	Releases prior to 15.1(3)MR are vulnerable; Releases 15.1(3)MR and later are not vulnerable.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1MRA	Not vulnerable	15.1(3)MRA2
15.1S	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(3)S6 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SG	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(2)SG1 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNI	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this

		advisory.
15.1SVD	Not vulnerable	Not vulnerable
15.1SVE	Not vulnerable	Not vulnerable
15.1SVF	Not vulnerable	Not vulnerable
15.1SY	Not vulnerable	15.1(1)SY2; Available on 28-OCT-13 15.1(2)SY
15.1T	Not vulnerable	Vulnerable; First fixed in Release 15.1M
15.1XO	Not vulnerable	Not vulnerable
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Bundled Publication**
There are no affected 15.2 based releases		
Affected 15.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Bundled Publication**
There are no affected 15.3 based releases		

* Cisco Catalyst 4500 Supervisor Engine 6-E/6L-E 搭載の Cisco Catalyst 4500 シリーズ スイッチは、 Cisco IOS ソフトウェア リリース 15.1SG に移行できます。

Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェアは、このアドバイザリで説明した脆弱性の影響を受けます。

Cisco IOS XE Software Release	First Fixed Release	First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication
2.1.x	Vulnerable; migrate to 3.3.0S or later.	Vulnerable; migrate to 3.4.6S or later.
2.2.x	Vulnerable; migrate to 3.3.0S or later.	Vulnerable; migrate to 3.4.6S or later.
2.3.x	Vulnerable; migrate to 3.3.0S or later.	Vulnerable; migrate to 3.4.6S or later.
2.4.x	Vulnerable; migrate to 3.3.0S or later.	Vulnerable; migrate to 3.4.6S or later.
2.5.x	Vulnerable; migrate to 3.3.0S or later.	Vulnerable; migrate to 3.4.6S or later.
2.6.x	Vulnerable	Vulnerable; migrate to 3.4.6S or

	; migrate to 3.3.0S or later.	later.
3.1.xS	Vulnerable; migrate to 3.3.0S or later.	Vulnerable; migrate to 3.4.6S or later.
3.1.xSG	Vulnerable; migrate to 3.3.0SG or later.	Vulnerable; migrate to 3.4.1SG or later.
3.2.xS	Vulnerable; migrate to 3.3.0S or later.	Vulnerable; migrate to 3.4.6S or later.
3.2.xSE	Not vulnerable	3.2.3SE
3.2.xSG	Vulnerable; migrate to 3.3.0SG or later.	Vulnerable; migrate to 3.4.1SG or later.
3.2.xXO	Vulnerable; migrate to 3.3.0XO or later.	Vulnerable; migrate to 3.3.0XO or later.
3.2.xSQ	Vulnerable; migrate to 3.3.0SQ or later.	Vulnerable; migrate to 3.3.0SQ or later.
3.3.xS	3.3.0S	Vulnerable; migrate to 3.4.6S or later.
3.3xSG	Not vulnerable	Vulnerable; migrate to 3.4.1SG or later.
3.3.xXO	Not vulnerable	Not vulnerable
3.3.xSQ	Not vulnerable	Not vulnerable
3.4.xS	Not vulnerable	3.4.6S
3.4.xSG	Not vulnerable	3.4.1SG *
3.5.xS	Not vulnerable	Vulnerable; migrate to 3.7.4S or later.
3.5.xE	Not vulnerable	Not vulnerable
3.6.xS	Not vulnerable	Vulnerable; migrate to 3.7.4S or later.
3.7.xS	Not vulnerable	3.7.4S

3.8.xS	Not vulnerable	Vulnerable; migrate to 3.9.2S or later.
3.9.xS	Not vulnerable	3.9.2S
3.10.xS	Not vulnerable	Not vulnerable

* Cisco Catalyst 4500 Supervisor Engine 7-E/7L-E 搭載の Cisco Catalyst 4500 シリーズ スイッチ、および Cisco Catalyst 4500-X シリーズ スイッチは、 Cisco IOS XE ソフトウェア リリース 3.4SG に移行できます。

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、『 Cisco IOS XE 2 Release Notes』、『 Cisco IOS XE 3S Release Notes』、『 Cisco IOS XE 3SG Release Notes』を参照してください。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、このアドバイザリで説明されている脆弱性の影響は受けません。

回避策

他のマルチキャスト ドメインからのマルチキャスト NTP トラフィックを必要としないお客様は、MSDP ピアからのNTP マルチキャスト グループへのトラフィックをドロップするよう MSDP SA フィルタを設定することが可能です。次の例は、アドレス 10.54.54.54 で設定されている MSDP ピアからデバイスに送信されるすべての MSDP トラフィックに適用される MSDP SA フィルタを示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
```

注：以前の MSDP SA フィルタは、デバイスに設定されている 1 つ 1 つの MSDP ピアに適用する必要があり、特定の環境に従ってカスタマイズが必要です。

MSDP SA フィルタに関する推奨事項の詳細は、http://www.cisco.com/en/US/tech/tk828/technologies_tech_note09186a0080093fda.shtml を参照してください。

修正済みソフトウェアの入手

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。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

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、ご購入いただいたフィーチャ 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、アクセスまたはその他の方法で使用した場合、お客様は

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、 Cisco.com の Software Navigator からアップグレードを入手することができます。 http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

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、お客様のケースの対応中に発見されました。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ntp

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2013-September-25	Initial public release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。