# Cisco IOSソフトウェアのマルチキャストネット ワークタイムプロトコルにおけるDoS脆弱性

High

アドバイザリーID: cisco-sa-20130925-ntp CVE-2013-

初公開日: 2013-09-25 16:00 5472

バージョン 1.0 : Final CVSSスコア : 7.1

回避策: No Workarounds available

Cisco バグ ID: CSCuc81226

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該当デバイスのリロードを引き起こし、その結果、サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、設定済みMSDPピアからのMulticast Source Discovery Protocol(MSDP)Source-Active(SA)メッセージにカプセル化された該当デバイスに送信されるマルチキャストNTPパケットの不適切な処理に起因します。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する可能性があります。この脆弱性が繰り返し悪用されると、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 軽減する回避策があります。

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-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 Cisco Security Advisoryが含まれています。すべてのアドバイザリは、Cisco IOSソフトウェアの 脆弱性に対処しています。各Cisco IOSソフトウェアセキュリティアドバイザリには、このアドバイザリで説明されている脆弱性を修正したCisco IOSソフトウェアリリースと、2013年9月のバンドル公開に含まれるすべてのCisco IOSソフトウェアの脆弱性を修正したCisco IOSソフトウェア リリースが記載されています。

個々の公開リンクは、次のリンクの「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

#### 脆弱性のある製品

該当するCisco IOSソフトウェアリリースを実行しているシスコデバイスは、次の2つの条件が満たされると脆弱になります。

- デバイス設定には、マルチキャストNTP設定コマンドが含まれます
- デバイスに少なくとも1つのMSDPピアが設定されている

デバイスが前述の条件を満たしているかどうかを判断するには、次の手順を使用できます。

NAT が設定にあるかどうかを判断するには、脆弱性がある次の設定例に示すように show running-config | include ^interface|ntp multicast特権EXECコマンドを使用すると、デバイス設定にマルチキャストNTP設定コマンドが含まれているかどうかを確認できます。次に、 show running-config | include ^interface|ntp multicastコマンドを、マルチキャストNTP用に設定された複数のインターフェイスを持つCisco IOSソフトウェアが稼働するデバイスで実行した場合の出力例を示します。

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:デバイスの設定にマルチキャストNTPコマンドがない場合は、次の手順をスキップできます。このデバイスには脆弱性はありません。

show ip msdp summary特権EXECコマンドを使用すると、デバイスに少なくとも1つの MSDPピアが設定されているかどうかを確認できます。次に、MSDPピアが1つ設定された Cisco IOSソフトウェアを実行しているデバイスで show ip msdp summaryコマンドを実行した 場合の出力を示します。

Router#show ip msdp summary MSDP Peer Status Summary

10.54.54.54 ?

Peer Address AS State Uptime/ Reset SA Peer Name
Downtime Count Count

Up

Downtime Count Count 00:35:03 0 6 ?

Router#

MSDPピアが設定されていないデバイスは脆弱ではありません。

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て show version コマンドを使って、システム バナーを表示します。"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。

次の例は、シスコ製品がCisco IOSソフトウェアリリース15.0(1)M1を実行し、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。

#### <#root>

Router>

show version

Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE 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

!--- output truncated

Cisco IOSソフトウェアのリリース命名規則の追加情報は、次のリンクの『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を参照。

脆弱性を含んでいないことが確認された製品

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 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

NTPは、マシンのネットワークの時刻を同期するように設計されています。NTPはUDP上で動作し、IP上で転送されます。NTPを実行しているネットワークデバイスは、参照時刻源と時刻を同期する際に、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。ネットワークデバイスは、2つの方法でネットワークの時刻情報を取得できます。1つはホストサーバにポーリングを行う方法、もう1つはNTPブロードキャストを受信する方法です。

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該当デバイスのリロードを引き起こし、その結果、サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、設定済みMSDPピアからのMulticast Source Discovery Protocol(MSDP)Source-Active(SA)メッセージにカプセル化された該当デバイスに送信されるマルチキャストNTPパケットの不適切な処理に起因します。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する可能性があります。この脆弱性が繰り返し悪用されると、DoS 状態が続く可能性があります。

この脆弱性は、Cisco Bug ID <u>CSCuc81226</u> (<u>登録</u> 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。

### 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ピアから送信されてNTPマルチキャストグループに送信されるトラフィックをドロップするようにMSDP SAフィルタを設定できます。次の例は、アドレス10.54.54.54の設定済み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

```
access-list 111 remark -- Deny traffic from any source to the NTP multicast group access-list 111 deny ip any host 224.0.1.1 access-list 111 remark -- Allow everything else access-list 111 permit ip any any
```

ip msdp sa-filter in 10.54.54.54 list 111

注:以前のMSDP SAフィルタは、デバイスで設定されたすべてのMSDPピアに適用する必要があり、特定の環境に応じてカスタマイズする必要があります。

MSDP SAフィルタリングの推奨事項の詳細については、

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

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 のシスコ セキュ リティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の 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。

### Cisco IOS ソフトウェア

次のCisco IOSソフトウェアテーブルの各行は、Cisco IOSソフトウェアトレインに対応しています。特定のトレインに脆弱性が存在する場合、修正を含む最も古いリリースが「最初の修正済みリリース」列に表示されます。2013年9月のバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリースには、Cisco IOSソフトウェアセキュリティアドバイザリのバンドル公開に含まれるすべての公開済みの脆弱性を修正する最初の修正リリースが記載されています。可能な場合は、利用可能な最新のリリースにアップグレードすることをお勧めします。

Cisco IOS Software Checkerを使用すると、特定のCisco IOSソフトウェアリリースに対応するシスコセキュリティアドバイザリを検索できます。このツールは、Cisco Security(SIO)ポータル (<a href="https://sec.cloudapps.cisco.com/security/center/selectIOSVersion.x">https://sec.cloudapps.cisco.com/security/center/selectIOSVersion.x</a>)で利用できます。

メジャー リ リース	修正済みリリ・	一スの入手可能性
Affected 12.0-Based Releases	First Fixed Release(修正された最初の リリース)	2013年9月のバンドル公開に含まれるすべてのアドバイザリに対する最初の修正 リリース
12.0S		脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。
12.0SY	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。

12.0SZ   脆弱性が存在します。このアドバイザリ	
12.2-Based Release       First Fixed Release (修正された最初の リリース)       べてのアドバイザリに対する最初の修 リリース         注:12.2(58)EXより前のリリースには脆弱性あり。最初の修正はリリース         12.2FX       弱性があり、12.2(58)EX以降のリリース	識に
12 2FX   弱性があり、12 2(58)FX以降のリリース   腕弱性あり。最初の修正は <u>リリース</u>	
には脆弱性はありません。	
注:12.2(58)EYより前のリリースには脆 弱性があり、12.2(58)EY以降のリリース には脆弱性はありません。	
注:12.2(58)EZより前のリリースには脆 弱性があり、12.2(58)EZ以降のリリース には脆弱性はありません。 12.2(60)EZ2より前のリリースには脆! 性があり、12.2(60)EZ2以降のリリーご には脆弱性はありません。最初の修正 リリース15.0SE	-ス
12.2IRB 脆弱性あり。最初の修正は <u>リリース</u> 脆弱性あり。最初の修正は <u>リリース</u> 12.2SRE <u>12.2SRE</u>	
12.2IRC 脆弱性あり。最初の修正は <u>リリース</u> 脆弱性あり。最初の修正は <u>リリース</u> <u>12.2SRE</u> <u>12.2SRE</u>	
12.2IRD   脆弱性あり。最初の修正は <u>リリース</u>   脆弱性あり。最初の修正は <u>リリース</u>   12.2SRE   12.2SRE	
12.2IRE 脆弱性あり。最初の修正は <u>リリース</u> 脆弱性あり。最初の修正は <u>リリース</u> 12.2SRE 12.2SRE	
12.2IRF   脆弱性あり。最初の修正は <u>リリース</u>   脆弱性あり。最初の修正は <u>リリース</u>   12.2SRE   12.2SRE	
12.2IRG 脆弱性が存在します。このアドバイザリ 脆弱性が存在します。このアドバイサ の「 <u>修正済みソフトウェアの取得</u> 」セク の「 <u>修正済みソフトウェアの取得</u> 」セク ションの手順に従って、サポート組織に ションの手順に従って、サポート組織 お問い合わせください。	セク
12.2IRH 脆弱性が存在します。このアドバイザリ 脆弱性が存在します。このアドバイサ の「 <u>修正済みソフトウェアの取得</u> 」セク の「 <u>修正済みソフトウェアの取得</u> 」セク ションの手順に従って、サポート組織に ションの手順に従って、サポート組織 お問い合わせください。	セク
12.2IRI 脆弱性が存在します。このアドバイザリ 脆弱性が存在します。このアドバイサ の「 <u>修正済みソフトウェアの取得</u> 」セク の「 <u>修正済みソフトウェアの取得</u> 」セ ションの手順に従って、サポート組織に お問い合わせください。	セク 織に 
┃12.2IXG   ┃脆弱性が存在します。このアドバイザリ ┃脆弱性が存在します。このアドバイサ	<u>ザリ</u>

	î	1
	の「修正済みソフトウェアの取得」セク	の「修正済みソフトウェアの取得」セク
	ションの手順に従って、サポート組織に お問い合わせください。	ションの手順に従って、サポート組織に お問い合わせください。
	<del>                                     </del>	
		脆弱性が存在します。このアドバイザリーの「 <u>修正済みソフトウェアの</u> 取得」セク
12.2IXH	ションの手順に従って、サポート組織に	の <u>  『正月ペプノドフェナの取得</u> 」 ピラ    ションの手順に従って、サポート組織に
	お問い合わせください。	プログの子順に促って、ケホート温順に    お問い合わせください。
	<u> </u>	脆弱性あり。最初の修正はリリース
12.2MC	移行	加切け。取切り停止は <u>りり ス</u> 15.1M
	脆弱性あり。最初の修正は <u>リリース</u>	<u> </u>
12.2MRA	12.2SRE	加切にあり。取物の修正は <u>クラース</u> 12.2SRE
	<del>-</del>	<del>IZ.ZSINL</del> 脆弱性が存在します。このアドバイザリ
		応羽性が存在します。このアドハイリリー  の「 <u>修正済みソフトウェアの</u> 取得」セク
12.2MRB		の
	お問い合わせください。	プョンの子順に促って、ケホート組織に    お問い合わせください。
12.2SB	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	·
12.256	12.2(33)SB15	12.2(33)SB15
12.2SCA	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
	12.2SCH	12.2SCH
12.2SCB	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
	12.2SCH	<u>12.2SCH</u>
12.2SCC	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
12.2000	<u>12.2SCH</u>	<u>12.2SCH</u>
12.2SCD	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
12.2000	<u>12.2SCH</u>	<u>12.2SCH</u>
12.2SCE	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
12.23CE	<u>12.2SCH</u>	<u>12.2SCH</u>
40.0005	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
12.2SCF	<u>12.2SCH</u>	<u>12.2SCH</u>
40.0000	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
12.2SCG	<u>12.2SCH</u>	<u>12.2SCH</u>
12.2SCH	12.2(33)SCH1	12.2(33)SCH1
	12.2(55)SE8	
12.2SE	12.2(58)SE	12.2(55)SE8
40.00==	脆弱性あり。15.0SEの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>
12.2SEG	移行	15.0SE
12.2SG	12.2(53)SG10(2013年12月に入手可能 <u>)*</u>	   12.2(53)SG10(2013年12月に入手可能 <u>)*</u>
12.2SGA	, , , , , , , , , , , , , , , , , , , ,	脆弱性が存在します。このアドバイザリ

		1
	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
12.2SM	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.25101	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
12.2SQ	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.23Q	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
40.000	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
12.2SRA	<u>12.2SRE</u>	<u>12.2SRE</u>
40.00DD	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
12.2SRB	<u>12.2SRE</u>	<u>12.2SRE</u>
40.0000	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
12.2SRC	<u>12.2SRE</u>	<u>12.2SRE</u>
40.00DD	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
12.2SRD	12.2SRE	<u>12.2SRE</u>
12.2SRE	12.2(33)SRE9	12.2(33)SRE9
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
40.0075	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.2STE	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
40.00\/	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.2SV	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
40.00\/D	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.2SVD	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
40.00\/E	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.2SVE	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
40.00\4/	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>
12.2SW	移行	<u>15.1M</u>
12.2SXF	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
•		

	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	プョンの子順に従って、リホート組織に  お問い合わせください。	プョンの子順に従って、リホート組織に    お問い合わせください。
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
12.2SXH	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.25/11	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
12.2SXI	12.2(33)SXI12	12.2(33)SXI12
12.2日本語	脆弱性なし	12.2(33)SXJ6
12.2SY	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
12.251	<u>15.0SY</u>	<u>15.0SY</u>
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
12.2WO	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.200	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
40 0 0 0 0 0 0	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」
12.2XNA	を参照してください。	を参照してください。
40 OVND	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」
12.2XNB	を参照してください。	を参照してください。
12.2XNC	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」
IZ.ZANC	を参照してください。	を参照してください。
12.2XND	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」
IZ.ZAND	を参照してください。	を参照してください。
12.2XNE	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」
IZ.ZANL	を参照してください。	を参照してください。
12.2XNF	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」	「 <u>Cisco IOS XEソフトウェアの可用性</u> 」
IZ.ZANF	を参照してください。	を参照してください。
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
12.2XO	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.280	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
12.27\/	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.2ZYA	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
Affected	Eiret Eivod Pologoo / 修正された早知の	2013年9月のバンドル公開に含まれるす
12.3-Based	First Fixed Release(修正された最初の	べてのアドバイザリに対する最初の修正
Releases	リリース )	リリース
12.3BC	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
IZ.JDU	<u>12.2SCH</u>	<u>12.2SCH</u>
<del></del>	•	*

	1	i
12.3JEC	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
		の「 <u>修正済みソフトウェアの取得</u> 」セク
	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
12.3JED	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
12.3JEE	┃ ┃脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u>
12.33LL	ING 33 IT AS O	<u>15.1M</u>
	75 77 M. A.	脆弱性あり。最初の修正は <u>リリース</u>
12.3JX	脆弱性なし	<u>15.1M</u>
	脆弱性あり。最初の修正は <u>リリース</u>	脆弱性あり。最初の修正は <u>リリース</u>
12.3XI	12.2SB	12.2SB
40.0V.I	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>
12.3XJ	移行	<u>15.1M</u>
	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>
12.3XK	移行	<u>15.1M</u>
	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正はリリース
12.3XL	移行	15.1M
	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正はリリース
12.3XQ	移行	15.1M
	脆弱性あり。15.0Mの任意のリリースに	<del>□□□</del> 脆弱性あり。最初の修正はリリース
12.3XR	移行	15.1M
	脆弱性あり。15.0Mの任意のリリースに	<u> </u>
12.3XU	移行	15.1M
	脆弱性あり。15.0Mの任意のリリースに	
12.3XW		脆弱性あり。最初の修正は <u>リリース</u>   15 1M
	移行	15.1M
12.3XX	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>
	移行	<u>15.1M</u>
12.3YD	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>
12.010	移行	<u>15.1M</u>
40.07/	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>
12.3YF	移行	<u>15.1M</u>
10.01.5	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>
12.3YG	移行	15.1M
	脆弱性あり。15.0Mの任意のリリースに	 脆弱性あり。最初の修正は <u>リリース</u>
12.3YI	移行	加速場  上の・ケ。 東   のの   多正   の <u>ラック   ス</u>   15.1M
12.3YJ	1	10:11W
12.313	IDLUMITED リット人に	ᄧᄳᅜᇷᄄᅅᇅᇮ ᄧᄭᄱᆙᅂᄄᅛ <u>ᆺᇧᅩᄉ</u>

	移行	<u>15.1M</u>
12.3YK	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.3YM	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.3YQ	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.3YS	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.3YT	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.3YU	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.3YX	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.3YZ	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。
12.3ZA	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
Affected 12.4-Based Releases	First Fixed Release(修正された最初の リリース)	2013年9月のバンドル公開に含まれるす べてのアドバイザリに対する最初の修正 リリース
12.4	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4GC	脆弱性なし	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JA	脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4JAL	脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u> <u>12.4JAM</u>
12.4ジャム	脆弱性なし	12.4(25e)JAM2
12.4JAN	脆弱性なし	脆弱性なし
12.4JAX	脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4JAZ	脆弱性なし	脆弱性が存在します。このアドバイザリ

12.4JDA   脆弱性なし   脆弱性なし   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   脆弱性が存在します。このアドバイザリカ・変をあり。最初の修正はリリース   15.1M   脆弱性なし   脆弱性なり。最初の修正はリリース   15.1M   脆弱性なり。最初の修正はリリース   15.1M   脆弱性なし   脆弱性なり。最初の修正はリリース   15.1M   12.4JZ   脆弱性なり。最初の修正はリリース   15.1M   12.4JZ   脆弱性なり。最初の修正はリリース   15.1M   12.4JZ   12.4JZ   12.4JZ   12.4JZ   12.4JZ   12.4JZ   12.4JZ   12.4JZ   13.4Z   13.4Z   14.4Z			
お問い合わせください。   施弱性な			の「 <u>修正済みソフトウェアの取得</u> 」セク
脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性あり。最初の修正はリリース   12.4JHC   脆弱性なし   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   12.4JK   12.4JK   12.4JK   12.4JK   12.4JK   13.51M   13.51M   13.51M   14.51M   14.51M   15.51M   15.5			ションの手順に従って、サポート組織に
12.4JDA 脆弱性なし の「修正済みソフトウエアの取得」セクションの手順に従って、サポート組織にお問い合わせください。 腕弱性が存在します。このアドバイザリの「修正済みソフトウエアの取得」セクションの手順に従って、サポート組織にお問い合わせください。 腕弱性なし の「修正済みソフトウエアの取得」セクションの手順に従って、サポート組織にお問い合わせください。 腕弱性なり 一名 15.1M 腕弱性が存在します。このアドバイザリの「修正済みソフトウエアの取得」セクションの手順に従って、サポート組織にお問い合わせください。 腕弱性が存在します。このアドバイザリの「修正済みソフトウエアの取得」セクションの手順に従って、サポート組織にお問い合わせください。 腕弱性が存在します。このアドバイザリの「修正済みソフトウエアの取得」セクションの手順に従って、サポート組織にお問い合わせください。 腕弱性が存在します。このアドバイザリの「修正済みソフトウエアの取得」セクションの手順に従って、サポート組織にお問い合わせください。 腕弱性が存在します。このアドバイザリの「修正済みソフトウエアの取得」セクションの手順に従って、サポート組織にお問い合わせください。 腕弱性が存在します。このアドバイザリの「修正済みソフトウエアの取得」セクションの手順に従って、サポート組織にお問い合わせください。 腕弱性が存在します。このアドバイザリの「修正済みソフトウエアの取得」セクションの手順に従って、サポート組織にお問い合わせください。 腕弱性なり 最初の修正はリリース 15.1M 腕弱性あり。最初の修正はリリース 15.1M			お問い合わせください。
12.4JDA   脆弱性なし   ションの手順に従って、サポート組織に   お問い合わせください。   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織に   お問い合わせください。   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織に   お問い合わせください。   脆弱性なし   12.4JDE   脆弱性なし   12.4JHA   脆弱性なし   12.4JHA   脆弱性なし   12.4JHA     脆弱性なし   12.4JHB     12.4JHB   12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB   12.4JHB   12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB   12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB     12.4JHB   12.4JHB     12.4JHB			脆弱性が存在します。このアドバイザリ
12.4JDC   脆弱性なし   加弱性なし   加弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   加弱性なり。最初の修正はリリース   15.1M   脆弱性なし   加弱性なし   加弱性なし   加弱性なし   加弱性などださい。   12.4JHA   加弱性なし   加弱性などが多数に対している。   12.4JHA   加弱性なし   加弱性などが多数に対している。   12.4JHB   加弱性なし   加弱性などが多数に対している。   12.4JHB   加弱性なし   加弱性などが存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   12.4JHC   加弱性なし   加弱性なし   12.4JK   加弱性なし   加弱性などが存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   12.4JK   加弱性なし   加弱性などが存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   12.4JK   加弱性なし   12.4JK   加弱性なし   12.4JK   加弱性なし   13.1M   加弱性なり。最初の修正はリリース   15.1M   12.4JY   加弱性なり   15.1M   12.4JY   15.1M   12.4JY   15.1M   12.4JY   15.1M   12.4JY   15.1M   12.4JY   15.1M   12.4JY   12.4JY   15.1M   12.4JY   12.4JY   12.4JY   12.4JY   12.4JY   13.1M   13.4JY   13.4JY   14.4JY   14.4JY   14.4JY   14.4JY   14.4JY   15.1M   14.4JY	12 4 10 4	마 <del>스</del> 크리 사ナ ナァ I	の「 <u>修正済みソフトウェアの取得</u> 」セク
脆弱性なし   脆弱性なし   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   脆弱性なり。最初の修正はリリース   15.1M   脆弱性なし   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   15.1M   脆弱性なし   15.1M   脆弱性なし   15.1M   15.	12.4JDA	加羽注なし	ションの手順に従って、サポート組織に
12.4JDC   脆弱性なし			お問い合わせください。
12.4JDC   脆弱性なし   ションの手順に従って、サポート組織に お問い合わせください。   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セク ションの手順に従って、サポート組織に お問い合わせください。   脆弱性なし   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セク ションの手順に従って、サポート組織に お問い合わせください。   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セク ションの手順に従って、サポート組織に お問い合わせください。   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セク ションの手順に従って、サポート組織に お問い合わせください。   脆弱性なし   脆弱性なり。最初の修正は リリース   15.1M   脆弱性なし   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」 セク ションの手順に従って、サポート組織に お問い合わせください。   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セク ションの手順に従って、サポート組織に お問い合わせください。   脆弱性なし   脆弱性なり。最初の修正は   リース   12.4JX   脆弱性なし   脆弱性あり。最初の修正は   リース   15.1M   脆弱性なし   脆弱性あり。最初の修正は   リース   15.1M   脆弱性なし   脆弱性あり。最初の修正は   リース   15.1M   脆弱性なし   脆弱性あり。最初の修正は   リース   15.1M   脆弱性あり。最初の修正は   リース   15.1M   脆弱性あり。最初の修正は   リリース   15.1M     脆弱性あり。最初の修正は   リリース   15.1M     脆弱性なし     脆弱性あり。最初の修正は   リリース   15.1M			脆弱性が存在します。このアドバイザリ
12.4JDD   脆弱性なし   ションの手順に従って、サポート組織に お問い合わせください。   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セク ションの手順に従って、サポート組織に お問い合わせください。   脆弱性あり。最初の修正はリリース   12.4JHA   脆弱性なし   12.4JHA   12.4JHB   12.4JHB   12.4JHB   12.4JHB   12.4JHB   12.4JHB   12.4JHC   12.	40.4100	면 크고 사사 ナン I	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.4JDD   脆弱性なし   脆弱性が存在します。このアドバイザリッ「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   脆弱性なし   鬼初の修正はリリース   15.1M   脆弱性なし   節弱性なし   元子の取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性あり。最初の修正はリリース   12.4JHC   脆弱性なし   元子の取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   鬼初の修正はリリース   15.1M   脆弱性なし   脆弱性なり。最初の修正はリリース   15.1M   1	12.4JDC	肥物性なし	ションの手順に従って、サポート組織に
12.4JDD       脆弱性なし       の「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。         12.4JDE       脆弱性なし       脆弱性あり。最初の修正はリリース         15.1M       脆弱性なします。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。         12.4JHB       脆弱性なし       ションの手順に従って、サポート組織にお問い合わせください。         12.4JHC       脆弱性なし       ションの手順に従って、サポート組織にお問い合わせください。         12.4JK       脆弱性なし       ・修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。         12.4JL       脆弱性なし       ・の「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。         12.4JX       脆弱性なし       ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・			お問い合わせください。
12.4JDD   脆弱性なし   ションの手順に従って、サポート組織にお問い合わせください。   脆弱性なり。最初の修正はリリース   15.1M   脆弱性なし   脆弱性なりを回じて、サポート組織にお問い合わせください。   脆弱性なし   からします。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   からします。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   脆弱性なり。最初の修正はリリース   15.1M   脆弱性なし   脆弱性なし   12.4JK   脆弱性なし   12.4JL   脆弱性なし   12.4JL   脆弱性なし   12.4JL   脆弱性なし   12.4JL   脆弱性なし   12.4JL     脆弱性なし   12.4JX     脆弱性なし   12.4JX     脆弱性なし   12.4JX     脆弱性なし   12.4JX     脆弱性なし   12.4JX     脆弱性なし   13.1M     13			脆弱性が存在します。このアドバイザリ
12.4JDE   脆弱性なし   脆弱性なし   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   加弱性なり   の「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   脆弱性なり。最初の修正はリリース   15.1M   脆弱性なし   脆弱性なし   12.4JK   脆弱性なし   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   脆弱性なし   12.4JL   脆弱性なし   脆弱性なり。最初の修正はリリース   15.1M   12.4JX   脆弱性なし   脆弱性あり。最初の修正はリリース   15.1M   脆弱性なし   脆弱性あり。最初の修正はリリース   15.1M   15.	40 4100	75 33 LL & 1	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.4JDE   脆弱性なし   脆弱性あり。最初の修正は <u>リリース 15.1M</u>   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織に お問い合わせください。   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織に お問い合わせください。   脆弱性なし   脆弱性あり。最初の修正は <u>リリース 15.1M</u>   脆弱性なし   脆弱性なし   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織に お問い合わせください。   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織に お問い合わせください。   脆弱性なし   脆弱性なり。最初の修正は <u>リリース 15.1M</u>   脆弱性なり。最初の修正は <u>リリース 15.1M</u>   脆弱性なし   脆弱性あり。最初の修正は <u>リリース 15.1M</u>   脆弱性なし   脆弱性あり。最初の修正は <u>リリース 15.1M</u>   脆弱性あり。最初の修正は   1.2.4JY   脆弱性なし   脆弱性あり。最初の修正は   1.2.4JY   脆弱性なし   脆弱性あり。最初の修正は   1.2.4JY   1.2.	12.4JDD	肥物性なし	ションの手順に従って、サポート組織に
12.4JDE   脆弱性なし   15.1M   12.4JHA   脆弱性なし   15.1M   12.4JHA   脆弱性なし   15.1M   12.4JHA   脆弱性なし   15.1M   12.4JHB   脆弱性なし   12.4JHB   脆弱性なし   12.4JHB   脆弱性なし   12.4JHB   12.4JHC   13.4HHC   14.4HHC   15.4HHC   15.4			お問い合わせください。
15.1M   脆弱性なし   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なり。最初の修正は <u>リリース   15.1M   脆弱性なし   脆弱性が存在します。このアドバイザリの「<u>修正済みソフトウェアの取得</u>」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「<u>修正済みソフトウェアの取得</u>」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「<u>修正済みソフトウェアの取得</u>」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   脆弱性なり。最初の修正は<u>リリース   15.1M</u>   脆弱性なり。最初の修正は<u>リリース   15.1M</u>   脆弱性なり。最初の修正は<u>リリース   15.1M</u>   脆弱性あり。最初の修正は<u>リリース   15.1M</u>   脆弱性あり。最初の修正は<u>リリース   15.1M</u>     脆弱性あり。最初の修正は<u>リリース   15.1M</u>                                      </u>			脆弱性あり。最初の修正はリリース
12.4JHA   脆弱性なし   の「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   の「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   脆弱性なり。最初の修正は <u>リリース 15.1M</u>   脆弱性なし   脆弱性なし   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   売品を対して、サポート組織にお問い合わせください。   脆弱性なし   売品を対したさせください。   脆弱性なり。最初の修正は <u>リリース 15.1M</u>   脆弱性なり。最初の修正は <u>リリース</u>	12.4JDE	脆弱性なし 	15.1M
12.4JHA   脆弱性なし   の「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   の「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   脆弱性なり。最初の修正は <u>リリース 15.1M</u>   脆弱性なし   脆弱性なし   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   売品を対して、サポート組織にお問い合わせください。   脆弱性なし   売品を対したさせください。   脆弱性なり。最初の修正は <u>リリース 15.1M</u>   脆弱性なり。最初の修正は <u>リリース</u>			脆弱性が存在します。このアドバイザリ
12.4JHA   脆弱性なし   ションの手順に従って、サポート組織に お問い合わせください。   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セク ションの手順に従って、サポート組織に お問い合わせください。   脆弱性なし   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セク ションの手順に従って、サポート組織に お問い合わせください。   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セク ションの手順に従って、サポート組織に お問い合わせください。   脆弱性が存在します。このアドバイザリ の「修正済みソフトウェアの取得」セク ションの手順に従って、サポート組織に お問い合わせください。   脆弱性あり。最初の修正は リリース 15.1M   脆弱性なし   脆弱性あり。最初の修正は リリース 15.1M			
お問い合わせください。   脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性あり。最初の修正はリリース	12.4JHA	脆弱性なし	
12.4JHB   脆弱性なし   の「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   12.4JHC   脆弱性なし   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   の「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   12.4JX   脆弱性なし   脆弱性あり。最初の修正は <u>リリース</u> 15.1M   脆弱性あり。最初の修正は <u>リリース</u> 15.1M   脆弱性あり。最初の修正は <u>リリース</u> 15.1M   12.4JY   脆弱性なし   15.1M   15.1M   15.1M   15.1M			
12.4JHB   脆弱性なし   の「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   12.4JHC   脆弱性なし   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性なし   の「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   12.4JX   脆弱性なし   脆弱性あり。最初の修正は <u>リリース</u> 15.1M   脆弱性あり。最初の修正は <u>リリース</u> 15.1M   脆弱性あり。最初の修正は <u>リリース</u> 15.1M   12.4JY   脆弱性なし   15.1M   15.1M   15.1M   15.1M			脆弱性が存在します。このアドバイザリ
12.4JHB       脆弱性なし       ションの手順に従って、サポート組織にお問い合わせください。         12.4JHC       脆弱性なし       脆弱性あり。最初の修正はリリース         15.1M       脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。         12.4JL       脆弱性なし       脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。         12.4JX       脆弱性なし       脆弱性あり。最初の修正はリリース         15.1M       脆弱性なり。最初の修正はリリース         15.1M       脆弱性あり。最初の修正はリリース         15.1M       脆弱性なり。最初の修正はリリース			
お問い合わせください。   12.4JHC   脆弱性なし   脆弱性あり。最初の修正は <u>リリース 15.1M</u>   脆弱性なし   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   12.4JX   脆弱性なし   脆弱性あり。最初の修正は <u>リリース 15.1M</u>   脆弱性なし   脆弱性あり。最初の修正は <u>リリース 15.1M</u>   脆弱性なし   12.4JY   脆弱性なし   15.1M	12.4JHB	脆弱性なし	
12.4JHC     脆弱性なし       12.4JK     脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。       12.4JL     脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。       12.4JX     脆弱性なし       12.4JY     脆弱性なし       12.4JY     脆弱性なし			
12.4JHC     脆弱性なし       12.4JK     脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。       12.4JL     脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。       12.4JX     脆弱性なし       12.4JY     脆弱性なし       12.4JY     脆弱性なし			
12.4JK   脆弱性なし   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   12.4JX   脆弱性なし   脆弱性あり。最初の修正は <u>リリース</u> 15.1M   脆弱性あり。最初の修正は <u>リリース</u> 15.1M   脆弱性あり。最初の修正は <u>リリース</u> 15.1M	12.4JHC	脆弱性なし	
12.4JK脆弱性なしの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。12.4JL脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。12.4JX脆弱性なし12.4JX脆弱性なし12.4JY脆弱性あり。最初の修正はリリース15.1M12.4JY脆弱性なし			
12.4JK       脆弱性なし       ションの手順に従って、サポート組織にお問い合わせください。         12.4JL       脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。         12.4JX       脆弱性なし       脆弱性あり。最初の修正はリリース15.1M         12.4JY       脆弱性なし       脆弱性あり。最初の修正はリリース15.1M			
お問い合わせください。   お問い合わせください。   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   12.4JX   脆弱性なし   脆弱性あり。最初の修正は <u>リリース15.1M</u>   脆弱性なし   脆弱性あり。最初の修正は <u>リリース15.1M</u>	12.4JK	脆弱性なし	
12.4JL   脆弱性なし   脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。   脆弱性あり。最初の修正は <u>リリース</u>			
12.4JL脆弱性なしの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。12.4JX脆弱性あり。最初の修正は <u>リリース</u> 15.1M12.4JY脆弱性あり。最初の修正は <u>リリース</u> 15.1M			
12.4JL脆弱性なしションの手順に従って、サポート組織にお問い合わせください。12.4JX脆弱性あり。最初の修正は <u>リリース</u> 15.1M12.4JY脆弱性あり。最初の修正は <u>リリース</u> 15.1M			
お問い合わせください。  12.4JX 脆弱性なし 脆弱性あり。最初の修正は <u>リリース</u> 15.1M  12.4JY 脆弱性なし 脆弱性あり。最初の修正は <u>リリース</u> 15.1M	12.4JL	脆弱性なし	
12.4JX脆弱性なし脆弱性あり。最初の修正は <u>リリース</u> 15.1M12.4JY脆弱性なし脆弱性あり。最初の修正は <u>リリース</u> 15.1M			
12.4JX     脆弱性なし       12.4JY     脆弱性なし       15.1M       15.1M			
12.4JY 脆弱性なし 脆弱性あり。最初の修正は <u>リリース</u> 15.1M	12.4JX	脆弱性なし	
12.4JY 脆弱性なし 15.1M			
<u>15.1M</u>	12.4JY	  脆弱性なし	
12.4JZ 脆弱性なし 脆弱性あり。最初の修正は <u>リリース</u>			<u>15.1M</u>
	12.4JZ	脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u>

		<u>15.1M</u>
12.4MD	注:12.4(22)MDより前のリリースには脆弱性があり、12.4(22)MD以降のリリースには脆弱性はありません。	脆弱性あり。最初の修正は <u>リリース</u> <u>12.4MDB</u>
12.4MDA	脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u> <u>12.4MDB</u>
12.4MDB	脆弱性なし	12.4(24)MDB15
12.4MR	注:12.4(20)MRより前のリリースには脆弱性があり、12.4(20)MR以降のリリースには脆弱性はありません。	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。
1240万	脆弱性なし	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。
12.4MRB	脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4SW	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4T	注:12.4(20)Tより前のリリースには脆弱性があり、12.4(20)T以降のリリースには脆弱性はありません。	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4XA	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4XB	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4XC	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4XD	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4XE	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4XF	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4XG	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4XJ	脆弱性あり。15.0Mの任意のリリースに 移行	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
12.4XK	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>

	移行	<u>15.1M</u>
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
12.4XL	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.47.	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
12.4XM	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>
12.4AIVI	移行	<u>15.1M</u>
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
40.4701	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.4XN	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
40.4\/D	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.4XP	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
10.00	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>
12.4XQ	移行	<u>15.1M</u>
	注:12.4(22)XRより前のリリースには脆	
12.4XR	弱性があり、12.4(22)XR以降のリリース	肥弱性あり。最初の修正は <u>リリース</u>
	には脆弱性はありません。	<u>15.1M</u>
10 1) (=	施弱性あり。15.0Mの任意のリリースに	  脆弱性あり。最初の修正は <u>リリース</u>
12.4XT	移行	<u>15.1M</u>
	脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
40.404	の「 <u>修正済みソフトウェアの取得</u> 」セク	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.4XV	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
10 1301	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正は <u>リリース</u>
12.4XW	移行	<u>15.1M</u>
	脆弱性あり。15.0Mの任意のリリースに	脆弱性あり。最初の修正はリリース
12.4XY	移行	 15.1M
		脆弱性あり。最初の修正はリリース
12.4XZ	脆弱性なし	15.1M
		脆弱性あり。最初の修正はリリース
12.4YA	脆弱性なし	15.1M
		<del></del> 
	脆弱性なし	の「修正済みソフトウェアの取得」セク
12.4YB		ションの手順に従って、サポート組織に
		お問い合わせください。
		脆弱性が存在します。このアドバイザリ
12.4YD	脆弱性なし	の「修正済みソフトウェアの取得」セク
		12

No.		
		ションの手順に従って、サポート組織に
		お問い合わせください。
12.4YE	  脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u>
12.41		<u>15.1M</u>
		脆弱性が存在します。このアドバイザリ
10.47/0	마순 근로 사는 수 ၂	の「 <u>修正済みソフトウェアの取得</u> 」セク
12.4YG	脆弱性なし 	ションの手順に従って、サポート組織に
		お問い合わせください。
影響を受ける	First Fixed Dalages / 修正された見切の	2013年9月のバンドル公開に含まれるす
15.0 ベース	First Fixed Release(修正された最初の	べてのアドバイザリに対する最初の修正
のリリース	リリース )	リリース
15.0EA	脆弱性なし	15.0(2)EA1
	76 77 W. A. I	脆弱性あり。15.2Eの任意のリリースに
15.0EB	脆弱性なし 	
		脆弱性あり。15.2Eの任意のリリースに
15.0EC	脆弱性なし 	
		注:15.0(2)ED1より前のリリースには脆
15.0ED	  脆弱性なし	弱性があり、15.0(2)ED1以降のリリース
		には脆弱性はありません。
15.0EH	脆弱性なし	脆弱性なし
15.0EJ	<del> </del>	脆弱性なし
	Cisco IOS XEデバイス:「 <u>Cisco IOS</u>	Cisco IOS XEデバイス:「 <u>Cisco IOS</u>
15.0EX	XEソフトウェアの可用性」を参照して	XEソフトウェアの可用性」を参照して
	ください。	ください。
15.0EY	<del>                                     </del>	15.0(2)EY2
15.0EZ	  脆弱性なし	┃ ┃脆弱性が存在するのは、リリース
		15.0(2)EZだけです
		<u> </u>
15.0M	脆弱性なし	15.1M
	┃ ┃脆弱性が存在します。このアドバイザリ	脆弱性が存在します。このアドバイザリ
		の「修正済みソフトウェアの取得」セク
15.0MR	ションの手順に従って、サポート組織に	ションの手順に従って、サポート組織に
	お問い合わせください。	お問い合わせください。
		脆弱性あり。最初の修正は <u>リリース</u>
15.0秒	Cisco IOS XEデバイス:「 <u>Cisco IOS</u>	15.1S
	XEソフトウェアの可用性」を参照して	Cisco IOS XEデバイス:「 <u>Cisco IOS</u>
	ください。	<u>XEソフトウェアの可用性</u> 」を参照して
		ください。
<u>I</u>	L	<u> </u>

15.0SE	脆弱性なし	15.0(2)SE4
15.0SG	Cisco IOS XEデバイス:「 <u>Cisco IOS</u> <u>XEソフトウェアの可用性</u> 」を参照して ください。	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。 Cisco IOS XEデバイス:「 <u>Cisco IOS</u> XEソフトウェアの可用性」を参照してください。
15.0SQA	Cisco IOS XEデバイス:「 <u>Cisco IOS</u> <u>XEソフトウェアの可用性</u> 」を参照して ください。	Cisco IOS XEデバイス:「 <u>Cisco IOS</u> <u>XEソフトウェアの可用性</u> 」を参照して ください。
15.0SQB	Cisco IOS XEデバイス:「 <u>Cisco IOS</u> <u>XEソフトウェアの可用性</u> 」を参照して ください。	Cisco IOS XEデバイス:「 <u>Cisco IOS</u> <u>XEソフトウェアの可用性</u> 」を参照して ください。
15.0SY	15.0(1)SY3	15.0(1)SY5
15.0XA	脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
15.0XO	の「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。 Cisco IOS XEデバイス:「 <u>Cisco IOS</u> XEソフトウェアの可用性」を参照してください。
影響を受ける 15.1 ベース のリリース	First Fixed Release(修正された最初の リリース)	2013年9月のバンドル公開に含まれるす べてのアドバイザリに対する最初の修正 リリース
15.1EY	脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u> <u>15.2S</u>
15.1GC	脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>
1,510万	脆弱性なし	15.1(4)M7
15.1MR	15.1(3)MRより前のリリースには脆弱性 があり、15.1(3)MR以降のリリースには 脆弱性はありません。	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。
15.1MRA	脆弱性なし	15.1(3)MRA2
15.1S	Cisco IOS XEデバイス:「 <u>Cisco IOS</u>	15.1(3)S6

	<u>XEソフトウェアの可用性</u> 」を参照して ください。	Cisco IOS XEデバイス:「 <u>Cisco IOS</u> <u>XEソフトウェアの可用性</u> 」を参照して ください。		
15.1SG	Cisco IOS XEデバイス:「 <u>Cisco IOS</u> <u>XEソフトウェアの可用性</u> 」を参照して ください。	15.1(2)SG1 Cisco IOS XEデバイス:「 <u>Cisco IOS</u> <u>XEソフトウェアの可用性</u> 」を参照して ください。		
15.1SNG	脆弱性なし	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。		
15.1SNH	脆弱性なし	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。		
15.1SNI	脆弱性なし	脆弱性が存在します。このアドバイザリの「 <u>修正済みソフトウェアの取得</u> 」セクションの手順に従って、サポート組織にお問い合わせください。		
15.1SVD	脆弱性なし	脆弱性なし		
15.1SVE	脆弱性なし	脆弱性なし		
15.1SVF	脆弱性なし	脆弱性なし		
15.1SY	脆弱性なし	15.1(1)SY2(2013年10月28日に入手可能) 15.1(2)SY		
15.1T	脆弱性なし	脆弱性あり。最初の修正は <u>リリース</u> <u>15.1M</u>		
15.1XO	脆弱性なし	脆弱性なし		
Affected 15.2-Based Releases	First Fixed Release(修正された最初の リリース)	2013年9月のバンドル公開に含まれるす べてのアドバイザリに対する最初の修正 リリース		
	影響を受ける 15.2 ベースのリリー	ースはありません。		
Affected 15.3-Based Releases	First Fixed Release(修正された最初の リリース)	2013年9月のバンドル公開に含まれるす べてのアドバイザリに対する最初の修正 リリース		
影響を受ける 15.3 ベースのリリースはありません。				

<sup>\*</sup> Cisco Catalyst 4500 Supervisor Engines 6-Eまたは6L-Eを搭載したCisco Catalyst 4500シリーズスイッチは、 <u>Cisco IOSソフトウェアリリース15.1SG</u>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されている脆弱性の影響を受けます。

Cisco IOS XE ソフト ウェア リ リース	First Fixed Release(修正 された最初のリ リース)	2013年9月の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含まれるすべてのアドバイザリに対する最初の修正リリース
2.1.x	脆弱性あり。 3.3.0S以降に移 行してください 。	脆弱性あり。3.4.6S以降 に移行してください。
2.2.x	脆弱性あり。 3.3.0S以降に移 行してください 。	脆弱性あり。3.4.6S以降 に移行してください。
2.3.x	脆弱性あり。 3.3.0S以降に移 行してください 。	脆弱性あり。3.4.6S以降 に移行してください。
2.4.x	脆弱性あり。 3.3.0S以降に移 行してください 。	脆弱性あり。3.4.6S以降 に移行してください。
2.5.x	脆弱性あり。 3.3.0S以降に移 行してください 。	脆弱性あり。3.4.6S以降 に移行してください。
2.6.x	脆弱性あり。 3.3.0S以降に移 行してください 。	脆弱性あり。3.4.6S以降 に移行してください。
3.1.xS	脆弱性あり。 3.3.0S以降に移	脆弱性あり。3.4.6S以降 に移行してください。

	行してください	
	0	
3.1.xSG	脆弱性あり。 3.3.0SG以降に移 行してください 。	脆弱性あり。3.4.1SG以 降に移行してください。
3.2.xS	脆弱性あり。 3.3.0S以降に移 行してください 。	脆弱性あり。3.4.6S以降 に移行してください。
3.2.xSE	脆弱性なし	3.2.3SE
3.2.xSG	脆弱性あり。 3.3.0SG以降に移 行してください 。	脆弱性あり。3.4.1SG以 降に移行してください。
3.2.xXO	脆弱性あり。 3.3.0XO以降に移 行してください 。	脆弱性あり。3.3.0XO以 降に移行してください。
3.2.xSQ	脆弱性あり。 3.3.0SQ以降に移 行してください 。	脆弱性あり。3.3.0SQ以 降に移行してください。
3.3.xS	3.3.0S	脆弱性あり。3.4.6S以降 に移行してください。
3.3xSG	脆弱性なし	脆弱性あり。3.4.1SG以 降に移行してください。
3.3.xXO	脆弱性なし	脆弱性なし
3.3.xSQ	脆弱性なし	脆弱性なし
3.4.xS	脆弱性なし	3.4.6S
3.4.xSG	脆弱性なし	3.4.1SG <u>*</u>
3.5.xS	脆弱性なし	脆弱性あり。3.7.4S以降 に移行してください。
3.5.xE	脆弱性なし	脆弱性なし
3.6.xS	脆弱性なし	脆弱性あり。3.7.4S以降 に移行してください。

3.7.xS	脆弱性なし	3.7.4S	
3.8.xS	脆弱性なし	脆弱性あり。3.9.2S以降 に移行してください。	
3.9.xS	脆弱性なし	3.9.2S	
3.10.xS	脆弱性なし	脆弱性なし	

<sup>\*</sup> Cisco Catalyst 4500 Supervisor Engines 7-Eおよび7L-Eを搭載した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、 <u>Cisco IOS XEソフトウェアリリー</u>ス3.4SGに移行できます。

Cisco IOS ソフトウェア リリースへの Cisco IOS XE ソフトウェア リリースのマッピングについては、「<u>Cisco IOS XE 2 Release Notes</u>」、「<u>Cisco IOS XE 3S Release Notes</u>」、および「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を受けません

### 推奨事項

\$propertyAndFields.get("recommendations")

### 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。

この脆弱性は、お客様のケースのトラブルシューティング時に発見されました。

### **URL**

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ntp

### 改訂履歴

リビジョン 1.0	2013年9月25日	初版リリース
-----------	------------	--------

## 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。