Cisco IOSソフトウェアの侵入防御システムにおけるDoS脆弱性

アドバイザリーID : cisco-sa-20120926-ios-ips
CVE-2012-3950
初公開日 : 2012-09-26 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 : CSCtw55976

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ソフトウェアには、侵入防御システム(IPS)機能に脆弱性があり、特定のCisco IOS IPS設定が存在する場合、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ています。

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で確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-ios-ips

注：2012年9月26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9件のCisco Security Advisoryが含まれています。8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詳述された脆弱性を修正したCisco IOSソフトウェアリリースと、2012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: Semi-Annual 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_sep12.html

該当製品

脆弱性のある製品

Cisco IOS IPSが設定されているデバイスは、脆弱性のあるバージョンのCisco IOSソフトウェアを実行している特定のCisco IOS IPS設定に基づいて、この脆弱性の影響を受けます。

次の2つの条件の両方に該当する場合、デバイスの設定は影響を受けます。

1. Cisco IOS IPSの設定では、次のカテゴリのいずれかが有効になっています。
   - diag2（コンフィギュレーション内）
   - general_os（os内）
   - general_attack（attack内）
   - general_service（other_services内）
   - tcp（l2/l3/l4_protocol/ip内）
   - udp（l2/l3/l4_protocol/ip内）
   - dns(network_services)
   - 拡張（ios_ips内）
   - basic（ios_ips内）
   - past_releases（releases内）

   上記のカテゴリのいずれかが有効になっているかどうかを判断するには、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)コマンドshow ip ips configuration | ipsカテゴリCLI設定を開始します。 上記のカテゴリのいずれかが出力に含まれ、Enableフィールドの値がTrueの場合、そのカテゴリは有効になります。次の例は、デバイスでカテゴリbasicが有効になっているデバイスを示しています。

```
Router#show ip ips configuration | begin IPS Category CLI Configuration
IPS Category CLI Configuration:
    Category all:
        Retire: True
        Enable: False
    Category ios_ips basic:
        Retire: False
        Enable: True
    Category other_services:
        Retire: True
        Enable: False
```

2. 4つのIPSシグニチャ6054:0、6054:1、6062:0、6062:1がすべてコンパイルされていない場合。

4つのシグニチャがすべてコンパイルされているかどうかを判別するには、デバイスにログインし、CLIコマンド show ip ips signaturesを入力します | include 6054|6062を使用します。コンパイル済みステータス列(この例では3番目の列で、すべての列に Nr値があります)が Y以外の値を示す場合、シグニチャはコンパイルされません。 次の例は、4つすべてのシグニチャがデバイスでコンパイルされていないデバイスを示しています。

<#root>

```
Router#show ip ips signatures | include 6054|6062
  6062:1     N*

Nr

A      LOW     0     1    0    200   30  FA  N 100 S3
  6062:0     N*

Nr

A      LOW     0     1    0    200   30  FA  N 100 S3
  6054:1     N*

Nr

A      LOW     0     1    0    200   30  FA  N 100 S2
  6054:0     N*

Nr

A      LOW     0     1    0    200   30  FA  N 100 S2
```

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ません。

- Cisco IPS 4200 シリーズ センサー
- Cisco IPS 4300 シリーズ センサー
- Cisco ASA Advanced Inspection and Preventionセキュリティサービスモジュール
- 基本的なIPSサポートのためのCisco ASA IP監査
- Cisco Catalyst 6500シリーズ侵入検知システム
- Cisco IOSソフトウェアファイアウォール侵入検知システム

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

Cisco IOSソフトウェアにはサービス拒否(DoS)の脆弱性があり、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す可能性があります。

攻撃者は、該当するCisco IOS IPS設定を持つデバイスを介して正当なDNSパケットを送信することで、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、攻撃者は該当デバイスのリロードを引き起こす可能性があります。

この脆弱性は、Cisco Bug ID CSCtw55976(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-2012-3950が割り当てられています。

回避策

次の2つの対応策のいずれかにより、デバイスに対する脆弱性の不正利用が防止されます。

デバイスでDNSバージョン要求（6054/0および6054/1）およびDNS作成者要求（6062/0および6062/1）シグニチャを有効にする

6054または6062シグニチャのいずれかを有効にすると、不正利用が防止されます。 次の例は、4つすべてのシグニチャが有効になっていることを示しています。

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 6054 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#signature 6054 1
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#signature 6062 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#signature 6062 1
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#end
Do you want to accept these changes? [confirm]
```

Cisco IOS IPSのDNSインスペクションを無効にする

DNSトラフィックを検査しないようにCisco IOS IPSデバイスを設定するには、DNSトラフィックを拒否するIPS名にアクセスリストを接続します。 次の例は、IPS名に接続されたACLを示しています。このACLは、Cisco IOS IPSにDNSパケットを検査しないように指示しています。

```
Router#show running-config
<! output removed for brevity !>
!
ip ips name iosips list dont_inspect_dns
!
ip access-list extended dont_inspect_dns
 deny   udp any any eq domain
 deny   tcp any any eq domain
 remark <! Include other protocols that are not required to be inspected here !>
 permit ip any any
```

複数デバイス導入のためのCisco IOS IPSシグニチャセットの調整、導入、および更新についての詳細は、次のリンクを参照してください。
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/white_paper_c11_549300.htr

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 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。

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。2012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。シスコでは、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ています。

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(https://sec.cloudapps.cisco.com/security/center/selectIOSVersion.x)で利用できます。

メジャー リリース	修正済みリリースの入手可能性	
Affected 12.0-Based Releases	First Fixed Release（修正された最初のリリース）	2012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
該当する 12.0 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）	2012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
影響を受ける 12.2 ベースのリリースはありません。		
Affected 12.3-Based Releases	First Fixed Release（修正された最初のリリース）	2012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
12.3	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3B	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3BC	脆弱性なし	脆弱性なし
12.3BW	脆弱性なし	脆弱性なし

12.3JA	12.3(4)JA2より前のリリースには脆弱性があり、12.3(4)JA2以降のリリースには脆弱性はありません。12.4JAの任意のリリースに移行	12.3(4)JA2より前のリリースには脆弱性があり、12.3(4)JA2以降のリリースには脆弱性はありません。12.4JAの任意のリリースに移行
12.3JEA	脆弱性なし	脆弱性なし
12.3JEB	脆弱性なし	脆弱性なし
12.3JEC	脆弱性なし	脆弱性なし
12.3JED	脆弱性なし	脆弱性なし
12.3JEE	脆弱性なし	脆弱性なし
12.3JK	12.3(8)JK1より前のリリースには脆弱性があり、12.3(8)JK1以降のリリースには脆弱性はありません。12.3Tの任意のリリースに移行	12.3(2)JK3 までのリリースには脆弱性はありません。12.3(8)JK1以降のリリースには脆弱性はありません。最初の修正はリリース12.4
12.3JL	脆弱性なし	脆弱性なし
12.3JX	脆弱性なし	脆弱性なし
12.3T	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3TPC	脆弱性なし	12.3(4)TPC11a までのリリースには脆弱性はありません。
12.3VA	脆弱性なし	脆弱性なし
12.3XA	脆弱性なし	12.3(2)XA7より前のリリースには脆弱性があり、12.3(2)XA7以降のリリースには脆弱性はありません。最初の修正はリリース12.4
12.3XB	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。
12.3XC	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XD	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XE	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XF	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。
12.3XG	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XI	脆弱性なし	12.3(7)XI1b
12.3XJ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3XK	脆弱性なし	脆弱性あり。最初の修正はリリース12.4

12.3XL	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3XQ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XR	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XU	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T 12.3(8)XU1までのリリースには脆弱性はありません。
12.3XW	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3XX	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XY	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XZ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3YD	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YF	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YG	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YI	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YJ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YK	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YM	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YQ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YS	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YT	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YU	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YX	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3YZ	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。
12.3ZA	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）	2012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
12.4	脆弱性なし	12.4(25g)
12.4GC	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。
12.4JA	脆弱性なし	脆弱性なし
12.4JAL	脆弱性なし	脆弱性なし

12.4JAX	脆弱性なし	脆弱性なし
12.4ジェイ	脆弱性なし	脆弱性なし
12.4JDA	脆弱性なし	脆弱性なし
12.4JDC	脆弱性なし	脆弱性なし
12.4JDD	脆弱性なし	脆弱性なし
12.4JDE	脆弱性なし	脆弱性なし
12.4JHA	脆弱性なし	脆弱性なし
12.4JHB	脆弱性なし	脆弱性なし
12.4JHC	脆弱性なし	脆弱性なし
12.4JK	脆弱性なし	脆弱性なし
12.4JL	脆弱性なし	脆弱性なし
12.4JX	脆弱性なし	脆弱性なし
12.4JY	脆弱性なし	脆弱性なし
12.4JZ	脆弱性なし	脆弱性なし
12.4MD	脆弱性なし	12.4(24)MD7
12.4MDA	脆弱性なし	7600-SAMIでは12.4(24)MDA11 12.4(22)MDA6までのリリースには脆弱性はありません。
12.4MDB	脆弱性なし	12.4(24)MDB10
12.4MR	12.4(19)MR1より前のリリースには脆弱性があり、12.4(19)MR1以降のリリースには脆弱性はありません。 12.4MRAの任意のリリースに移行	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。
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「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。
12.4MRB	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4SW	脆弱性なし	脆弱性なし
12.4T	12.4(24)T8	12.4(24)T8
12.4XA	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XB	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XC	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XD	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XE	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XF	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T

12.4XG	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XJ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.4XK	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.4XL	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。
12.4XM	脆弱性なし	12.4(15)XMまでのリリースには脆弱性はありません。12.4(15)XM3以降のリリースには脆弱性はありません。最初の修正はリリース12.4T
12.4XN	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。
12.4XP	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。
12.4XQ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XR	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XT	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XV	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。
12.4XW	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.4XY	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.4XZ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.4YA	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.4YB	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。

12.4YD	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。
12.4YE	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4YG	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。
影響を受ける15.0 ベースのリリース	First Fixed Release（修正された最初のリリース）	2012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
15.0EX	脆弱性なし	脆弱性なし
15.0EY	脆弱性なし	脆弱性なし
15.0M	15.0(1)M9	15.0(1)M9
15.0MR	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。
15.0MRA	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。
15.0秒	脆弱性なし Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.0(1)S6 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.0SE	脆弱性なし	15.0(2)SE 15.0(2)SE1（12月10日に入手可能）
15.0SG	脆弱性なし Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.0(2)SG5 15.0(2)SG6（2012年10月11日に入手可能） Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.0SQA	脆弱性なし	脆弱性なし
15.0SY	脆弱性なし	15.0(1)SY2
15.0XA	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

15.0XO	脆弱性なし Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	脆弱性あり。最初の修正はリリース15.0SG Cisco IOS XEデバイス：「Cisco IOS 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）	2012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
15.1EY	脆弱性なし	15.1(2)EY4
15.1GC	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
1,510万	15.1(4)M5	15.1(4)M5
15.1MR	脆弱性なし	15.1(3)MR
15.1S	脆弱性なし Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.1(3)S3 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.1SG	脆弱性なし Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.1(1)SG1 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」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「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。
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「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。
15.1SNI	脆弱性なし	脆弱性あり。15.2SNGの任意のリリースに移行
15.1SV	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。
15.1T	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
15.1XB	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

Affected 15.2-Based Releases	First Fixed Release（修正された最初のリリース）	2012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
15.2GC	15.2(3)GCより前のリリースには脆弱性があり、15.2(3)GC以降のリリースには脆弱性はありません。最初の修正はリリース15.2T	15.2(3)GCより前のリリースには脆弱性があり、15.2(3)GC以降のリリースには脆弱性はありません。最初の修正はリリース15.2T
15.2JA	脆弱性なし	脆弱性なし
1,520万	脆弱性なし	15.2(4)M
15.2秒	脆弱性なし Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.2(1)S2 15.2(2)S1 15.2(4)S Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.2SNG	脆弱性なし	脆弱性なし
15.2T	15.2(1)T3 15.2(2)T2 15.2(3)T2（10月12日に入手可能）	15.2(1)T3 15.2(2)T2 15.2(3)T2（10月12日に入手可能）

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せん。

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、お客様のサポート要求を処理する際に発見されました。

URL

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

20120926-ios-ips

改訂履歴

リビジョン 1.0	2012年9月26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。