Cisco IOSソフトウェアのネットワークアドレス変換の脆弱性

アドバイザリーID : cisco-sa-20130925-nat
初公開日 : 2013-09-25 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 : CSCtq14817 CSCuf28733 CSCtn53730

CVE-2013-5479
CVE-2013-5481
CVE-2013-5480

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ソフトウェアに実装されているネットワークアドレス変換(NAT)機能には、IPパケットの変換時に3つの脆弱性があり、認証されていないリモートの攻撃者によってサービス妨害(DoS)状態が引き起こされる可能性があります。

シスコはこれら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。これらの脆弱性を軽減する回避策はありません。

このアドバイザリは、次のリンクより確認できます。

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

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

これらの脆弱性は、Cisco IOSソフトウェアの脆弱なバージョンを実行し、NATが設定されているデバイスに影響を与えます。

脆弱性のある製品

Cisco IOSソフトウェアを実行しているシスコデバイスは、NATが設定されている場合に脆弱性の影響を受けます。

デバイスにNATが設定されているかどうかを確認するには、次の2つの方法があります。

- デバイスでNATが有効になっているかどうかを確認します。
- デバイスの設定にNATコマンドが含まれているかどうかを確認します。

Cisco IOSデバイスでNATが有効になっているかどうかを確認するには、デバイスでNATが有効になっているかどうかを確認することをお勧めします。

デバイスでNATが有効になっているかどうかを確認する。

Cisco IOSソフトウェアの設定でNATが有効になっているかどうかを確認するには、デバイスにログインしてshow ip nat statisticsコマンドを発行します。NATがアクティブな場合、Outside interfacesとInside interfacesのセクションにはそれぞれ少なくとも1つのインターフェイスが含まれます。次の例は、NAT機能がアクティブになっているデバイスを示しています。

```
<#root>

Router#

 show ip nat statistics


Total translations: 2 (0 static, 2 dynamic; 0 extended)

Outside interfaces: Serial0
Inside interfaces: Ethernet1

Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool mypool refcount 2
 pool mypool: netmask 255.255.255.0
        start 192.168.10.1 end 192.168.10.254
        type generic, total addresses 14, allocated 2 (14%), misses 0
```

デバイスの設定にNATコマンドが含まれているかどうかの確認

また、Cisco IOSソフトウェアの設定でNATが有効になっているかどうかを判断するには、ip nat insideコマンドとip nat outsideコマンドの両方が異なるインターフェイスに存在している必要があります。NAT仮想インターフェイスの場合は、ip nat enableインターフェイスコマンドが存在します。

Cisco IOSソフトウェアリリースの判別

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

NAT機能が設定されていないCisco IOSデバイスは脆弱ではありません。

次の製品には脆弱性が存在しないことが確認されています。

- Cisco IOS XE ソフトウェア
- Cisco IOS XR ソフトウェア
- Cisco NX-OS ソフトウェア
- Cisco ASA 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

Cisco IOSソフトウェアのNAT機能には、3つの脆弱性が存在します。これらの脆弱性のうち2つはDNSパケットの変換に関係するもので、1つはPoint-to-Point Tunneling Protocol(PPTP)パケットの変換に関係するものです。これらの脆弱性はいずれも、3ウェイハンドシェイクを必要としません。

Cisco IOSソフトウェアのNAT DNSの脆弱性

Cisco IOSソフトウェアのDNS over TCPパケット機能のNATには2つの脆弱性があり、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れる可能性があります。この脆弱性は、特定の有効なDNS TCPストリームの不適切な処理に起因します。攻撃者は、TCPポート53で特定のDNSパケットを送信することにより、これらの脆弱性を不正利用する可能性があります。これらのDNSの脆弱性は、UDPポート53パケットを使用して不正利用したり、IPv6パケットを使用して不正利用したりすることはできません。

最初のNAT DNS脆弱性は、Cisco Bug ID CSCtn53730(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-2013-5479が割り当てられています。

2つ目のNAT DNS脆弱性は、Cisco Bug ID CSCuf28733(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-5480が割り当てられています。

注： RFC-5966 では、ゾーン転送以外のクエリのTCPトランスポートは、完全なDNSプロトコル実装の必須の部分であることが明記されています。TCPポート53を介したDNSの妨害は、意図しない結果を生む可能性があります。

Cisco IOSソフトウェアのNAT PPTPの脆弱性

Cisco IOSソフトウェアのPPTPパケットのNATには脆弱性があり、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れる可能性があります。この脆弱性は、特定の有効なPPTPパケットの不適切な処理に起因します。攻撃者は、TCPポート1723でPPTP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。

PPTPに対するNATは、TCPポート172およびIPプロトコル47の総称ルーティングカプセル化(GRE)パケットで実行されます。この脆弱性は、TCPポート1723のPPTPパケットを使用しての

み引き起こされます。

この脆弱性は、Cisco Bug ID CSCtq14817(登録ユーザ専用)として文書化され、CVE ID CVE-2013-5481が割り当てられています。

回避策

これらの脆弱性に対する回避策はありません。

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。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(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）	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
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）	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
12.2EX	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE

12.2EY	脆弱性なし	脆弱性あり。最初の修正はリリース15.2S
12.2EZ	脆弱性なし	12.2(60)EZ2より前のリリースには脆弱性があり、12.2(60)EZ2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15.0SE
12.2IRB	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRC	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRD	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRE	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRF	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRG	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。
12.2IRH	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。
12.2IRI	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。
12.2IXG	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。
12.2IXH	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。
12.2MC	脆弱性なし	脆弱性あり。最初の修正はリリース15.1M
12.2MRA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2MRB	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。
12.2SB	脆弱性なし	12.2(33)SB15
12.2SCA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCH
12.2SCB	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCH
12.2SCC	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCH
12.2SCD	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCH
12.2SCE	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCH
12.2SCF	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCH
12.2SCG	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCH
12.2SCH	脆弱性なし	12.2(33)SCH1
12.2SE	脆弱性なし	12.2(55)SE8
12.2SEG	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2SG	脆弱性なし	12.2(53)SG10(2013年12月に入手可能)*
12.2SGA	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。
12.2SM	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。
12.2SQ	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。
12.2SRA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRB	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRC	脆弱性なし	脆弱性あり。最初の修正はリリース

		12.2SRE
12.2SRD	脆弱性なし	脆弱性あり。最初の修正はリリース 12.2SRE
12.2SRE	脆弱性なし	12.2(33)SRE9
12.2STE	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。
12.2SV	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。
12.2SVD	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。
12.2SVE	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。
12.2SW	脆弱性なし	脆弱性あり。最初の修正はリリース15.1M
12.2SXF	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。
12.2SXH	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。
12.2SXI	脆弱性が存在するのは、リリース 12.2(33)SXI7だけです。	12.2(33)SXI12
12.2日本語	脆弱性が存在するのは、リリース 12.2(33)SXJ1だけです。	12.2(33)SXJ6
12.2SY	脆弱性あり。最初の修正はリリース 15.0SY 12.2(50)SY2までのリリースには脆弱性はありません。	脆弱性あり。最初の修正はリリース15.0SY
12.2WO	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。
12.2XNA	「Cisco IOS XEソフトウェアの可用性」を参照してください。	「Cisco IOS XEソフトウェアの可用性」を参照してください。
12.2XNB	「Cisco IOS XEソフトウェアの可用性」を参照してください。	「Cisco IOS XEソフトウェアの可用性」を参照してください。
12.2XNC	「Cisco IOS XEソフトウェアの可用性」を参照してください。	「Cisco IOS XEソフトウェアの可用性」を参照してください。
12.2XND	「Cisco IOS XEソフトウェアの可用性」を参照してください。	「Cisco IOS XEソフトウェアの可用性」を参照してください。
12.2XNE	「Cisco IOS XEソフトウェアの可用性」を参照してください。	「Cisco IOS XEソフトウェアの可用性」を参照してください。
12.2XNF	「Cisco IOS XEソフトウェアの可用性」を参照してください。	「Cisco IOS XEソフトウェアの可用性」を参照してください。
12.2XO	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。
12.2ZYA	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。
Affected 12.3-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
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）	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
該当する 12.4 ベースのリリースはありません。		
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）	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
15.0EA	脆弱性なし	15.0(2)EA1
15.0EB	脆弱性なし	脆弱性あり。15.2Eの任意のリリースに移行
15.0EC	脆弱性なし	脆弱性あり。15.2Eの任意のリリースに移行
15.0ED	脆弱性なし	注：15.0(2)ED1より前のリリースには脆弱性があり、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	脆弱性なし	脆弱性なし
15.0EX	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。	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。
15.0EY	脆弱性なし	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
15.0M	この脆弱性が存在するのは、リリース15.0(1)M6と15.0(1)M7だけです。	脆弱性あり。最初の修正はリリース15.1M
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。
15.0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。	脆弱性あり。最初の修正はリリース15.1S 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)SE4
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。	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。 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	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。	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。
15.0SQB	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。	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。
15.0SY	15.0(1)SY1	15.0(1)SY5
15.0XA	脆弱性なし	脆弱性あり。最初の修正はリリース15.1M
15.0XO	脆弱性なし	脆弱性が存在します。このアドバイザリの

	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。	「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。 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）	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。最初の修正はリリース15.2S
15.1GC	15.1(2)GC2までのリリースには脆弱性はありません。	脆弱性あり。最初の修正はリリース15.1M
1,510万	15.1(4)M7	15.1(4)M7
15.1MR	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。
15.1MRA	脆弱性なし	15.1(3)MRA2
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)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。
15.1SG	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(2)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。
15.1SVD	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	15.1(2)T5 15.1(2)T3までのリリースには脆弱性はありません。	脆弱性あり。最初の修正はリリース15.1M
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
15.2E	脆弱性なし	脆弱性なし
15.2GC	脆弱性あり。15.4Tの任意のリリースに移行	脆弱性あり。15.4Tの任意のリリースに移行
15.2JA	15.2(4)JA1	15.2(4)JA1
15.2JAX	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。
15.2JB	15.2(2)JB2	15.2(2)JB2
15.2JN	脆弱性なし	脆弱性なし
1,520万	15.2(4)M4	15.2(4)M4
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(4)S4 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。
15.2SA	脆弱性なし	15.2(2)SA
15.2SNG	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。
15.2SNH	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。
15.2SNI	脆弱性なし	脆弱性あり。最初の修正はリリース15.3S
15.2T	15.2(2)T4 15.2(3)T4	15.2(3)T4

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
1,530万	脆弱性なし	脆弱性なし
15.3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。	15.3(2)S2 15.3(3)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。
15.3T	15.3(1)T2 15.3(2)T1	15.3(1)T2 15.3(2)T1

* 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、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3件の脆弱性は、TACカスタマーサービスリクエストのトラブルシューティング中に発見されたものです。

URL

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

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

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。