1000シリーズアグリゲーションサービスルータ向けCisco IOS XEソフトウェアの複数の脆弱性

High

アドバイザリーID : cisco-sa-20130410-asr1000
初公開日 : 2013-04-15 16:00
最終更新日 : 2013-04-17 19:11
バージョン 1.3 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCtt11558 CSCtz23293 CSCub34945 CSCtz97563 CSCuc65609

CVE-2013-1165
CVE-2013-1164
CVE-2013-1167
CVE-2013-1166
CVE-2013-2779

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

1000シリーズアグリゲーションサービスルータ(ASR)用Cisco IOS XEソフトウェアには、次のサービス拒否(DoS)の脆弱性が存在します。

- Cisco IOS XEソフトウェアのIPv6マルチキャストトラフィックにおけるDoS脆弱性
- Cisco IOS XEソフトウェアのMVPNv6トラフィックにおけるDoS脆弱性
- Cisco IOS XEソフトウェアのL2TPトラフィックにおけるDoS脆弱性
- Cisco IOS XEソフトウェアのブリッジドメインインターフェイスにおけるDoS脆弱性
- Cisco IOS XEソフトウェアのSIPトラフィックにおけるDoS脆弱性

これらの脆弱性は互いに独立しています。いずれかの脆弱性の影響を受けるリリースが、他の脆弱性の影響を受けることはありません。

これらの脆弱性のいずれかが不正利用されると、認証されていないリモートの攻撃者によってEmbedded Services Processor(ESP)カードまたはRoute Processor(RP)カードのリロードが引き起こされ、サービスが中断され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。

注：Cisco IOSソフトウェアおよびCisco IOS-XRソフトウェアは、これらの脆弱性の影響を受けません。

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-20130410-asr1000

該当製品

1000シリーズASR向けCisco IOS XEソフトウェアには、複数のDoS脆弱性が存在します。1000シリーズASR向けCisco IOS XEソフトウェアの影響を受けるバージョンは、脆弱性によって異なります。影響を受けるバージョンの詳細については、このセキュリティアドバイザリの「ソフトウェアバージョンおよび修正」セクションを参照してください。

脆弱性のある製品

個々のバージョン情報については、このアドバイザリの「ソフトウェア バージョンおよび修正」セクションを参照してください。

Cisco IOS XEソフトウェアのIPv6マルチキャストトラフィックにおけるDoS脆弱性および
Cisco IOS XEソフトウェアのMVPNv6トラフィックにおけるDoS脆弱性

これらの脆弱性は、フラグメント化されたマルチキャストIPバージョン6(IPv6)またはフラグメント化されたIPv6マルチキャストVPN(MVPNv6)パケットが該当するCisco ASRデバイスで受信されたときに引き起こされます。Cisco Multicast Leaf Recycle Elimination(MLRE)によって処理されるフラグメント化されたマルチキャストパケットにより、Cisco ASRデバイス上のCisco ESPカードがリロードされる可能性があります。
Cisco ASR 1000に設定された複数の機能が、クラッシュを引き起こすこの種の処理をトリガーする可能性があります。

トラフィックを処理しているインターフェイスでIPv6が有効になっており、該当するデバイスでMLREが有効になっている場合、Cisco IOS XEソフトウェアが影響を受ける可能性があります。

インターフェイスでIPv6が有効になっているかどうかを確認するには、 show run | include ipv6.(enable|address) を使用することもできます。 ipv6 enableと ipv6 addressが show run | include ipv6.(enable|address)は、IPv6が有効であることを示します。
show runコマンドの出力を次に示します | include ipv6.(enable|address)コマンドを実行します。

```
asr1004# show run | include ipv6.(enable|address)
 ipv6 enable
 ipv6 address dhcp rapid-commit
 ipv6 address autoconfig
 ipv6 address MANAGEMENT ::1FFF:0:0:0:3560/128
 ipv6 address 2001:DB8::1/64
```

現在、デバイスでCisco MLREが有効になっているかどうかを判断する方法はありません。

注：Cisco MLRE機能は、Cisco IOS XEソフトウェアリリース3.4.1Sで導入され、エンベデッドサービスプロセッサ40(ASR1000-ESP40)またはエンベデッドサービスプロセッサ100(ASR1000-ESP100)を搭載したCisco ASR 1000シリーズアグリゲーションサービスルータ(ASR100)上のCisco IOS XEソフトウェアのすべてのバージョンで、デフォルトでででが有効になります。この脆弱性の影響を受けるのは、エンベデッドサービスプロセッサ40(ASR1000-ESP40)またはエンベデッドサービスプロセッサ100(ASR1000-ESP100)を搭載したCisco ASR 1000シリーズアグリゲーションサービスルータのみです。

Cisco ASR 1000デバイスにASR1000-ESP40またはASR1000-ESP100がインストールされているかどうかを確認するには、 show inventoryコマンドを発行します。エンベデッドサービスプロセッサ40(ASR1000-ESP40)を搭載したCisco ASR 1006ルータで実行されているCisco IOS XEソフトウェアでの show inventoryの出力を次に示します。

```
 asr1006#show inventory NAME: "Chassis", DESCR: "Cisco ASR1006
Chassis" PID: ASR1006 NAME: "module F1", DESCR: "Cisco ASR1000エンベデッドサービスプロセッサ， 40 Gbps" PID: ASR1000-ESP40 <output suppressed>
```

注：マルチキャストIPv6またはMVPNv6トラフィックを処理するように設定されているCisco IOSデバイスは、この脆弱性の影響を受けません。 該当するバージョンのCisco IOS XEソフトウェアを実行するCisco ASR 1000シリーズアグリゲーションサービスルータのみが、この脆弱性の影響を受けます。

Cisco IOS XEソフトウェアのL2TPトラフィックにおけるDoS脆弱性

Cisco IOS XEソフトウェアには、L2TP Network Server(LNS)終端またはL2TPv3イーサネット擬似回線(xconnect)が有効な場合に、特定のレイヤ2トンネリングプロトコル(L2TP)パケットを

大量に処理したときに、該当デバイスがリロードされる可能性のある脆弱性が存在します。 L2TP LNS終端およびxconnectは、デフォルトでは有効になっていません。

デバイスでL2TP LNS終端が有効になっているかどうかを確認するには、 show run | include accept-dialin特権EXECコマンドを使用します。 accept-dialinが show run | include accept-dialinは、L2TP LNS終端が有効になっていることを示します。

show runコマンドの出力を次に示します | include accept-dialinコマンドを、L2TPネットワークサーバ(LNS)として設定されているCisco IOS XEソフトウェアで実行した場合の出力例を示します。

```
asr1004#sho running-config | include accept-dialin
accept-dialin
```

デバイスでxconnectが有効になっているかどうかを確認するには、 show run | include xconnect|l2tpv3特権EXECコマンドを使用します。 encapsulation l2tpv3および xconnectが show run | include xconnect|l2tpv3はxconnectが有効であることを示します。

show runコマンドの出力を次に示します | include xconnect|l2tpv3コマンドを実行します。

<#root>

```
asr1004#sho running-config | include xconnect|l2tpv3
encapsulation l2tpv3
xconnect 10.0.0.1 1000 encapsulation l2tpv3 pw-class my_class
```

注:L2TPv3イーサネット擬似回線(xconnect)またはL2TP LNSとして設定されているCisco IOSデバイスは、この脆弱性の影響を受けません。 該当するバージョンのCisco IOS XEソフトウェアを実行するCisco ASR 1000シリーズアグリゲーションサービスルータのみが、この脆弱性の影響を受けます。

Cisco IOS XEソフトウェアのブリッジドメインインターフェイスにおけるDoS脆弱性

Cisco IOS XEソフトウェアには脆弱性があり、ブリッジドメインインターフェイス(BDI)機能が設定されている場合、パケットの処理中に該当デバイスがリロードされる可能性があります。

Cisco IOS XEソフトウェアは、次の条件がすべて満たされると、この脆弱性の影響を受ける可能性があります。

- 入力パスでパケットを処理する物理インターフェイスは、カプセル化タイプがタグなしに設定されているレイヤ3インターフェイスです。
- 着信パケットはBDIインターフェイスを介してルーティングされます。
- パケットの出力物理インターフェイスには、VLANを書き換えるように設定されたカプセル化があります。

注：BDI機能はデフォルトでは設定されていません。

デバイスで上記の条件が満たされているかどうかを確認するには、 show run | section interface特権EXECコマンドを使用します。 show runの出力を次に示します | 脆弱性のあるBDI設定が設定されたデバイス上のCisco IOS XEソフトウェアの section interface:

<#root>

```
 asr1004#sho running-config | section interface


interface GigabitEthernet0/0/3
        ip address 192.168.2.1 255.255.255.0

        !

interface BDI20

        ip address 192.168.1.1 255.255.255.0









 !


          interface GigabitEthernet0/0/4
        no ip address
        negotiation auto
        service instance 1 ethernet
        encapsulation dot1q 201

rewrite egress tag pop 1 symmetric
        bridge-domain 20
```

注：この機能は、Cisco IOS XEソフトウェアバージョン3.2.0SのCisco ASR 1000シリーズアグ

リゲーションサービスルータで導入されました。

注:BDIが設定されているCisco IOSデバイスは、この脆弱性の影響を受けません。 該当するバージョンのCisco IOS XEソフトウェアを実行するCisco ASR 1000シリーズアグリゲーションサービスルータのみが、この脆弱性の影響を受けます。

Cisco IOS XEソフトウェアのSIPトラフィックにおけるDoS脆弱性

Cisco IOS XEソフトウェアには、Virtual Routing and Forwarding(VRF)インスタンスおよびSIP Application Layer Gateway(ALG)インスペクションでネットワークアドレス変換(NAT)を受けるSession Initiation Protocol(SIP)パケットの処理中に、該当デバイスがリロードされる可能性のある脆弱性が存在します。攻撃者は、NATが設定されたデバイスを通過する大量のSIP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。

Cisco IOS XEソフトウェアは、該当するデバイスでVRF対応NATおよびSIP ALGが有効になっている場合、この脆弱性の影響を受ける可能性があります。これらのサービスはデフォルトでは有効になっていません。

SIP ALGは、NATが有効にされるとすぐにデバイスで有効になります。管理者は、NAT設定でSIP ALGインスペクションを無効にすることができます。

SIP ALGは、ゾーンベースポリシーファイアウォール(ZBFW)設定でも有効にできます。ZBFWでSIP ALGが設定されているデバイスは、この脆弱性の影響を受けません。

Cisco IOS XEソフトウェアの設定でVRF対応NATが有効になっているかどうかを判断するには、 ip nat insideコマンドまたは ip nat outsideコマンドが異なるインターフェイスに存在し、少なくとも1つの ip natグローバルコンフィギュレーションコマンドに vrfキーワードが含まれている必要があります。

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 ip(nat) | .* vrf .*)コマンドを使用すると、VRF対応NATが設定に存在するかどうかを確認できます。脆弱性のある次の設定例を参照してください。

<#root>

```
asr1004#show running-config | include ip (nat | .* vrf .*)
 ip nat inside
 ip nat outside
 ip nat inside source static 192.168.1.100 10.0.0.1
```

vrf

```
 VRF-SIP
```

出力が空の場合、特定のデバイスで実行されているCisco IOS XEソフトウェアリリースには脆弱性はありません。返された出力が空でない場合、SIP ALGサービスはNAT設定で明示的に無効にすることができます。NAT設定でSIP ALGが無効になっているかどうかを確認するには、show run | include ip nat 特権 EXEC コマンドを使用します。no ip nat service sipがshow run | include ip natの実行結果に出力される場合は、NATの設定でSIP ALGが無効になっていることを意味しています。

show runの出力を次に示します | include ip natコマンドを、NAT設定でSIP ALGが無効になっているCisco IOS XEソフトウェアで実行した場合の出力例を示します。

<#root>

```
asr1004#show running-config | include ip nat
 ip nat inside
 ip nat outside
 ip nat inside source static 192.168.1.100 10.0.0.1 vrf sip

no ip nat service sip udp port 5060
 no ip nat service sip tcp port 5060
```

no ip nat service sipが show run | include ip nat コマンドの実行結果に出力されない場合は、デバイスで実行されている Cisco IOS XE ソフトウェア リリースに脆弱性が存在することになります。

注:SIP ALGインスペクションが設定されているCisco IOSデバイスは、この脆弱性の影響を受けません。 該当するバージョンのCisco IOS XEソフトウェアを実行するCisco ASR 1000シリーズアグリゲーションサービスルータのみが、この脆弱性の影響を受けます。

実行ソフトウェア バージョンの判別

Cisco ASR 1000シリーズアグリゲーションサービスルータのIOS XEソフトウェアリリースは、Cisco IOSソフトウェアリリースに対応しています。たとえば、Cisco IOS XEソフトウェアリリース3.6.2Sは、Cisco ASR 1000シリーズアグリゲーションサービスルータIOSソフトウェアリリース15.2(2)S2のソフトウェアリリースです。
Cisco IOS XEソフトウェアリリースと関連するCisco IOSソフトウェアリリースとのマッピングの詳細については、次のドキュメントを参照してください。
http://www.cisco.com/en/US/docs/routers/asr1000/release/notes/asr1k_rn_intro.html

脆弱性のあるバージョンの IOS XE ソフトウェアがデバイスで実行されているかどうかを確認するには、show version コマンドを実行します。次の例は、IOS XEソフトウェアバージョン3.6.2S、IOSバージョン15.2(2)S2を実行しているCisco IOS XEソフトウェアを示しています。

```
asr1004#show version
Cisco IOS Software, IOS-XE Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.2(2)S2, RELEASE SO
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 07-Aug-12 13:40 by mcpre
<output suppressed>
```

注:Cisco IOS XEソフトウェアイメージは、サブパッケージとも呼ばれる7つの個別モジュールで構成されます。パッケージは、Cisco IOS XEソフトウェアのIn Service Software Upgrade(ISSU)機能を使用するように設計されています。お客様は、アップグレードが必要なパッケージのみをアップグレードできます。Cisco IOS XEソフトウェアパッケージの詳細については、次を参照してください。
http://www.cisco.com/en/US/partner/prod/collateral/routers/ps9343/product_bulletin_c25-448387.html

パッケージが個別にアップグレードされた場合、 show versionコマンドの出力が異なる場合があります。

脆弱性を含んでいないことが確認された製品

Cisco IOSソフトウェアまたはCisco IOS-XRソフトウェアを実行している製品は、これらの脆弱性の影響を受けません。

1000シリーズASR向けCisco IOS XEソフトウェアを除き、他のシスコ製品においてこれらの脆弱性の影響を受けるものは現在確認されていません。

詳細

次のセクションで、それぞれの脆弱性に関する追加情報を示します。

Cisco IOS XEソフトウェアのIPv6マルチキャストトラフィックにおけるDoS脆弱性

Cisco IOS XEソフトウェアには、認証されていないリモートの攻撃者がDoS状態を引き起こす可能性のある脆弱性が存在します。

この脆弱性は、ASR1000-ESP40またはASR1000-ESP100を搭載したCisco 1000シリーズASRに

よる、フラグメント化されたIPv6マルチキャストトラフィックの不適切な処理に起因します。 攻撃者は、フラグメント化されたIPv6マルチキャストパケットを、該当システムを通過する、または該当システム宛てに送信することで、この脆弱性を不正利用する可能性があります。

エクスプロイトに成功すると、攻撃者はシステムのリロードを引き起こし、その結果DoS状態が発生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 CSCtz97563(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-2013-1164が割り当てられています

Cisco IOS XEソフトウェアのMVPNv6トラフィックにおけるDoS脆弱性

Cisco IOS XEソフトウェアには、認証されていないリモートの攻撃者がDoS状態を引き起こす可能性のある脆弱性が存在します。

この脆弱性は、ASR1000-ESP40またはASR1000-ESP100を搭載したCisco 1000シリーズASRによる、フラグメント化されたIPv6 MVPNトラフィックの不適切な処理に起因します。攻撃者は、フラグメント化されたIPv6 MVPNパケットを、該当システムを通過する、または該当システム宛てに送信することで、この脆弱性を不正利用する可能性があります。

エクスプロイトに成功すると、攻撃者はシステムのリロードを引き起こし、その結果DoS状態が発生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 CSCub34945(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-2779が割り当てられています

Cisco IOS XEソフトウェアのL2TPトラフィックにおけるDoS脆弱性

Cisco IOS XEソフトウェアには、認証されていないリモートの攻撃者がDoS状態を引き起こす可能性のある脆弱性が存在します。

この脆弱性は、Cisco 1000 ASRによる特定のL2TPパケットの不適切な処理に起因します。攻撃者は、特定のL2TPパケットを大量に脆弱なシステムに送信することで、この脆弱性を不正利用する可能性があります。この脆弱性は、脆弱なデバイスを通過するL2TPトラフィックによってトリガーされることはありません。

エクスプロイトに成功すると、攻撃者はシステムのリロードを引き起こし、その結果DoS状態が発生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 CSCtz23293(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-1165が割り当てられています

Cisco IOS XEソフトウェアのブリッジドメインインターフェイスにおけるDoS脆弱性

Cisco IOS XEソフトウェアには、認証されていないリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性のある脆弱性が存在します。

この脆弱性は、 ブリッジドメインインターフェイス(BDI)用に設定されたCisco 1000シリーズASRによるパケットの不適切な処理に起因します。攻撃者は、該当システムを通過する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。この脆弱性は、脆弱性のあるデバイスにトラフィックを送信しても引き起こされません。

エクスプロイトに成功すると、攻撃者はシステムのリロードを引き起こし、その結果DoS状態が発生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 CSCtt11558(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-1167が割り当てられています

Cisco IOS XEソフトウェアのSIPトラフィックにおけるDoS脆弱性

Cisco IOS XEソフトウェアには、認証されていないリモートの攻撃者がDoS状態を引き起こす可能性のある脆弱性が存在します。

この脆弱性は、VRF対応NATおよびSIP ALG用に設定された場合に、Cisco 1000シリーズASRでSIPパケットが不適切に処理されることに起因します。攻撃者は、NATが設定されたデバイスを通過する大量のSIP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。この脆弱性は、脆弱性のあるデバイス宛てのSIPトラフィックによってトリガーされることはありません。

エクスプロイトに成功すると、攻撃者はシステムのリロードを引き起こし、その結果DoS状態が発生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 CSCuc65609(登録ユーザ専用)として文書化され、CVE ID CVE-2013-1166が割り当てられています。

回避策

これらの脆弱性を軽減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。

各Cisco IOS XEソフトウェアリリースは、標準サポートリリースまたは拡張サポートリリースのいずれかに分類されます。標準サポートリリースでは、エンジニアリングサポートの有効期間は1年で、リビルドは2回計画されています。延長サポートリリースでは、エンジニアリングサポートのライフタイムが合計2年、リビルドが4回計画されています。

Cisco IOS XEソフトウェアのサポート終了ポリシーおよび特定のCisco IOS XEソフトウェアリリースに関する関連サポートのマイルストーンの詳細については、次を参照してください。
http://www.cisco.com/en/US/prod/collateral/routers/ps9343/product_bulletin_c25-448258.html

Cisco IOS XEソフトウェアのIPv6マルチキャストトラフィックにおけるDoS脆弱性

脆弱性	メジャー リリース	拡張リリース	First Fixed Release（修正された最初のリリース）
0.CSCtz97563	2.x	-	Not affected
	3.1	Yes	Not affected
	3.2	いいえ	Not affected

	3.3	いいえ	Not affected
	3.4	Yes	3.4.4S
	3.5	いいえ	脆弱性あり。いずれかの拡張リリースに移行する
	3.6	いいえ	脆弱性あり。いずれかの拡張リリースに移行する
	3.7	Yes	Not affected
	3.8	いいえ	Not affected

Cisco IOS XEソフトウェアのMVPNv6トラフィックにおけるDoS脆弱性

脆弱性	メジャー リリース	拡張リリース	First Fixed Release (修正された最初のリリース)
0.CSCub34945	2.x	-	Not affected
	3.1	Yes	Not affected
	3.2	いいえ	Not affected
	3.3	いいえ	Not affected
	3.4	Yes	3.4.5S
	3.5	いいえ	脆弱性あり。いずれかの拡張リリースに移行する
	3.6	いいえ	脆弱性あり。いずれかの拡張リリースに移行する
	3.7	Yes	3.7.1S
	3.8	いいえ	Not affected

Cisco IOS XEソフトウェアのL2TPトラフィックにおけるDoS脆弱性

脆弱性	メジャー リリース	拡張リリース	First Fixed Release（修正された最初のリリース）
0.CSCtz23293	2.x	-	脆弱性あり。いずれかの拡張リリースに移行する
	3.1	Yes	脆弱性あり。いずれかの拡張リリースに移行する
	3.2	いいえ	脆弱性あり。いずれかの拡張リリースに移行する
	3.3	いいえ	脆弱性あり。いずれかの拡張リリースに移行する
	3.4	Yes	3.4.5S
	3.5	いいえ	脆弱性あり。いずれかの拡張リリースに移行する
	3.6	いいえ	脆弱性あり。いずれかの拡張リリースに移行する
	3.7	Yes	3.7.1S
	3.8	いいえ	Not affected

Cisco IOS XEソフトウェアのブリッジドメインインターフェイスにおけるDoS脆弱性

脆弱性	メジャー リリース	拡張リリース	First Fixed Release（修正された最初のリリース）
0.CSCtt11558	2.x	-	Not affected
	3.1	Yes	Not affected

	3.2	いいえ	脆弱性あり。いずれかの拡張リリースに移行する
	3.3	いいえ	脆弱性あり。いずれかの拡張リリースに移行する
	3.4	Yes	3.4.2S
	3.5	いいえ	脆弱性あり。いずれかの拡張リリースに移行する
	3.6	いいえ	Not affected
	3.7	Yes	Not affected
	3.8	いいえ	Not affected

Cisco IOS XEソフトウェアのSIPトラフィックにおけるDoS脆弱性

脆弱性	メジャー リリース	拡張リリース	First Fixed Release（修正された最初のリリース）
0.CSCuc65609	2.x	-	Not affected
	3.1	Yes	Not affected
	3.2	いいえ	Not affected
	3.3	いいえ	Not affected
	3.4	Yes	3.4.5S
	3.5	いいえ	Not affected
	3.6	いいえ	Not affected
	3.7	Yes	Not affected
	3.8	いいえ	Not affected

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。

推奨リリース

推奨リリースの表に、このアドバイザリの公開時点で公開済みのすべての脆弱性に対する修正が含まれているリリースを示します。次の表に示すリリース以降にアップグレードすることを推奨します。

影響を受けるリリース	推奨リリース	拡張リリース
2.x	脆弱性あり。推奨される拡張リリースのいずれかに移行してください。	-
3.1	脆弱性あり。推奨される拡張リリースのいずれかに移行してください。	Yes
3.2	脆弱性あり。推奨される拡張リリースのいずれかに移行してください。	いいえ
3.3	脆弱性あり。推奨される拡張リリースのいずれかに移行してください。	いいえ
3.4	3.4.5S	Yes
3.5	脆弱性あり。推奨される拡張リリースのいずれかに移行してください。	いいえ

3.6	脆弱性あり。推奨される拡張リリースのいずれかに移行してください。	いいえ
3.7	3.7.1S	Yes
3.8	脆弱性なし;	いいえ

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）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

Cisco IOS XEソフトウェアのブリッジドメインインターフェイスにおけるDoS脆弱性は、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ました。
その他の脆弱性は、シスコの社内テストで発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130410-asr1000

改訂履歴

リビジョン 1.3	2013年 4月17日	CVE割り当てを更新しました。MVPNv6脆弱性にCVE-2013-2779を再割り当てしました。
リビジョン 1.2	2013年 4月15日	SIP脆弱性に関するソフトウェアテーブルを更新
リビジョン 1.1	2013年 4月10日	「脆弱性のある製品」の「L2TPトラフィック」セクションにxconnectを追加。
リビジョン 1.0	2013年 4月10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。