Cisco Security Advisory: Multiple Vulnerabilities in Cisco IOS Software Traffic Optimization Features

Advisory ID: cisco-sa-20120328-mace

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

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 2012 March 28 16:00 UTC (GMT)

目次

要約

Cisco IOS ソフトウェアの Wide Area Application Services（WAAS）Express 機能には、認証されていないリモートの攻撃者がルータのメモリ リークまたは再起動を引き起こすことのできるサービス拒否（DoS）の脆弱性が含まれます。

また、Cisco IOS ソフトウェアの Measurement, Aggregation, and Correlation Engine（MACE）機能には、認証されていないリモートの攻撃者がルータのメモリ リークを引き起こすことのできる DoS 脆弱性が含まれます。

攻撃者は、WAAS Express または MACE が設定されたルータに対して通過トラフィックを送信することで、これらの脆弱性を不正利用することができます。これらの脆弱性の不正利用に成功した場合、認証されていないリモートの攻撃者はルータのメモリ リークまたは再起動を引き起こせる場合があります。また、不正利用が繰り返されることによって、長時間にわたる DoS 状態に陥る可能性があります。

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。このアドバイザリは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

注：2012 年 3 月 28 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。各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決する Cisco IOS ソフトウェア リリース、および 2012 年 3 月にバンドル公開したすべての脆弱性を解決する Cisco IOS ソフトウェア リリースを記載しています。

個々の公開リンクは、次のリンクにある「Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication」内に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

該当製品

脆弱性が存在する製品

Cisco IOS ソフトウェアを実行しているシスコ デバイスで、1 つ以上のインターフェイスに **mace enable** または **waas enable** インターフェイス コンフィギュレーション コマンドによる設定が行われている場合、そのデバイスには脆弱性が存在します。WAAS Express または MACE には、さらに設定が必要です。詳細は次で説明します。

注：Cisco IOS ソフトウェアは、WAAS Express または MACE が設定されている場合にのみ脆弱性があります。WAAS Express ではなく WAAS が設定されている Cisco IOS ソフトウェアは、この脆弱性の影響を受けません。

WAAS Express についての詳細は、 http://www.cisco.com/en/US/products/ps11211/index.html を参照してください。
MACE についての詳細は、
http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps11709/ps11671/guide_c07-664643.html を参照してください。

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

脆弱性が存在しない製品

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 Wide Area Application Services（WAAS）Express 機能は、 中央に配置されたアプリケーションにアクセスするための WAN の帯域を最適化します。 この WAAS Express を利用することで、他のデバイスを使用することなく Cisco サービス統合型ルータ（ISR G2）でトラフィックを最適化できます。

Cisco Measurement, Aggregation, and Correlation Engine（MACE）は、ネットワーク トラフィックの測定と分析に使用する Cisco IOS 機能です。この機能は、WAAS Express と併せて使用した場合には最適化されたトラフィックの詳細を確認することができ、単独で使用した場合にはアプリケーション パフォーマンスの測定が行えます。

Cisco IOS ソフトウェアの WAAS Express 機能には、認証されていないリモートの攻撃者がルータのメモリ リークまたは再起動を引き起こすことのできる DoS の脆弱性が含まれます。この脆弱性は、Cisco Bug ID CSCtt45381（ 登録ユーザのみ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2012-1314 が割り当てられています。

Cisco IOS ソフトウェアの MACE 機能には、認証されていないリモートの攻撃者がルータのメモリ リークまたは再起動を引き起こすことのできる DoS の脆弱性が含まれます。この脆弱性は、Cisco Bug ID CSCtq64987 および CSCtu57226 として文書化され、CVE ID CVE-2012-1312 が割り当てられています。

攻撃者は、WAAS Express または MACE が設定されたルータに対して通過トラフィックを送信することで、これらの脆弱性を不正利用することができます。これらの脆弱性の不正利用に成功した場合、認証されていないリモートの攻撃者はルータのメモリ リークまたはリロードを引き起こすことができます。また、不正利用が繰り返されることによって、長時間にわたる DoS 状態に陥る可能性があります。

次に抜粋した設定に類似する設定が 1 つ以上ある場合、WAAS Express または MACE が設定されたルータは脆弱性の影響を受けます。

次の例は、WAAS Express 設定の一部を示しています。 `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
```

次の例は、前の抜粋で示した WAAS Express の設定がすでに行われている場合の MACE 設定の

一部を示しています。

```
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次の例は、WAAS Express が設定されていない
場合の MACE 設定の一部を示しています。
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
```

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ 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導き出すことができます。

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、シスコは個々の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

CSCtt45381 Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	

Functional	Official-Fix	Confirmed

CSCtq64987 and CSCtu57226 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

これらの脆弱性の不正利用に成功した場合、認証されていないリモートの攻撃者はルータのメモリ リークまたはリロードを引き起こすことができます。また、不正利用が繰り返されることによって、長時間にわたる DoS 状態に陥る可能性があります。

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 and Responses アーカイブと、後続のアドバイザリを参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が不明確な場合は、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である場合、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 March 2012 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。シスコは利用可能な最新のリリースへのアップグレードを推奨します。

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）ポータルで入手できます。
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 March 20 Cisco IOS Software Security Advisory Bundled Publi
There are no affected 12.0 based releases		
Affected 12.2-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 20 Cisco IOS Software Security Advisory Bundled Publi
There are no affected 12.2 based releases		
Affected 12.3-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 20 Cisco IOS Software Security Advisory Bundled Publi
There are no affected 12.3 based releases		
Affected 12.4-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 20 Cisco IOS Software Security Advisory Bundled Publi
There are no affected 12.4 based releases		
Affected 15.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 20 Cisco IOS Software Security Advisory Bundled Publi
There are no affected 15.0 based releases		
Affected 15.1-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 20 Cisco IOS Software Security Advisory Bundled Publi
15.1EY	Not vulnerable	15.1(2)EY2
15.1GC	Not vulnerable	15.1(2)GC2
15.1M	15.1(4)M4; Available on 30-MAR-12	15.1(4)M4; Available on 30-MAR-12
15.1MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in section of this advisory.
15.1S	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS XE Sof Availability
15.1SG	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS XE Sof Availability
15.1SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in section of this advisory.
15.1SNH	Not vulnerable	Not vulnerable
15.1T	Not vulnerable	15.1(3)T3
15.1XB	Not vulnerable	Vulnerable; First fixed in
Affected 15.2-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 20 Cisco IOS Software Security Advisory Bundled Publi
15.2GC	15.2(1)GC2	15.2(1)GC2
15.2S	Not vulnerable	15.2(1)S1
15.2T	15.2(1)T2 15.2(2)T1 15.2(3)T; Available on 30-MAR-12	15.2(1)T2 15.2(2)T1 15.2(3)T; Available on 30-MAR-12

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 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は受けません。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、2012 年 3 月の Cisco IOS Software Security Advisory バンドル公開に含まれている脆弱性の影響を受けません。

回避策

この脆弱性に対する回避策はありません。

このアドバイザリに『Cisco Applied Mitigation Bulletin』（AMB）は付属していません。

```
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
```

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に特有の問題に関してご確認ください。

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。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 または http://www.cisco.com/public/sw-center/sw-usingswc.shtml 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。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

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 Center 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

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、適切な処置について支援を受けてく

ださい。

回避策の効果は、使用製品、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のお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とする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か、お客様のサービス プロバイダーやサポート会社にご相談ください。

サービス契約をご利用でないお客様

シスコから直接購入したが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、サードパーティ ベンダーから購入したが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を入手してください。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このアドバイザリの 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 を通して無償アップグレードをお求めください。

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を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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。

これらの脆弱性は、シスコの社内テストで発見されたものです。

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。またシスコシステムズ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-20120328-mace

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電子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

このアドバイザリに関する今後の更新があれば、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。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.0	2012-March-28	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支援、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について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。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。