Cisco IOS XE Software Network Address Translation Denial of Service Vulnerability

Advisory ID: cisco-sa-20150923-iosxe

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150923-iosxe

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 2015 September 23 16:00 UTC (GMT)

目次

要約

Cisco ASR 1000 シリーズ、Cisco ISR 4300 シリーズ、Cisco ISR 4400 シリーズ、および Cisco Cloud Services 1000v シリーズ ルータの Cisco IOS XE ソフトウェアのネットワーク アドレス変換 (NAT) サービスおよびマルチプロトコル ラベル スイッチング (MPLS) サービスを必要とする IPv4 パケット処理の脆弱性により、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のリロードが引き起こされる可能性があります。

この脆弱性は、NAT と MPLS の処理を必要とする IPv4 パケットの不適切な処理に起因します。攻撃者は、NAT サービスと MPLS サービスを実行するように設定された Cisco IOS XE デバイスが処理する IPv4 パケットを送信することにより、この脆弱性を不正利用する可能性があります。攻撃者はこの不正利用により、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。
シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 こ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、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150923-iosxe

注：2015 年 9 月 23 日、Cisco IOS ソフトウェアおよび IOS XE ソフトウェアのセキュリティ アドバイザリにおいて、3 つの Cisco Security Advisory を含むバンドル資料を公開しました。 これらのアドバイザリは Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの脆弱性を扱っています。 個々の公開リンクは次のリンクの『*Cisco Event Response: September 2015 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication*』を参照してください。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep15.html

該当製品

脆弱性が存在する製品

Cisco IOS XE ソフトウェアには、NAT サービスと MPLS サービスを必要とする IPv4 パケットを処理する際に該当するデバイスがリロードされる可能性のある脆弱性が含まれています。

この脆弱性が不正利用される可能性があるのは、IPv4 中継パケットのみです。 該当デバイスを宛先とするパケットまたは IPv6 パケットがこの脆弱性をトリガーすることはできません。 NAT サービスと MPLS サービスはデフォルトでは有効になっていません。

Cisco IOS XE ソフトウェアの設定で NAT が有効かどうかを判断するには、 **ip nat inside** コマンドまたは **ip nat outside** コマンドが別のインターフェイスに存在し、設定に少なくとも 1 つの **ip nat** グローバル コンフィギュレーション コマンドが必要です。

NAT が設定に存在す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|ip nat** コマンドを使用できます。

```
asr1000#show running-config | include ip nat
ip nat inside
ip nat outside
ip nat pool test 192.168.0.1 192.168.0.254 netmask 255.255.255.0
ip nat outside source list 1 pool test
```

出力が空白の場合、そのデバイスで稼働する Cisco IOS XE ソフトウェア リリースに脆弱性はありません。 出力が空白でない場合、Cisco IOS XE デバイス上で NAT が有効になっています。

Cisco IOS XEソフトウェアで MPLS が有効かどうかを判断するには、少なくとも 1 つのインターフェイスに **mpls ip** コマンド存在している必要があります。

設定に MPLS が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|mpls ip** コマンドを使用できます。

```
asr1000#show running-config | include mpls ip
mpls ip
```

さらに、 **ip nat outside** が設定されたインターフェイスに **mpls ip** コンフィギュレーション コマンドが存在していて、もう 1 つのインターフェイスの設定に **nat inside** コンフィギュレーション コマンドが存在している必要があります。 **show running-config interface** コマンドは以下の判断をするために使用できます。

- 設定の **ip nat outside** コマンドと同じインターフェイスに **mpls ip** コマンドがあるかどうか
- **ip nat inside** コマンドがもう 1 つのインターフェイスの設定にあるかどうか

次に脆弱性のある設定例を示します。

```
asr1000# show running-config interface
!
interface GigabitEthernet0/0
no shutdown
ip address 10.86.194.60 255.255.254.0
  ip nat inside
 !
interface GigabitEthernet0/1
no shutdown
ip address 10.10.4.200 255.255.0.0
  ip nat outside
mpls ip
 !
```

脆弱性が存在しない製品

Cisco IOS ソフトウェアは、この脆弱性の影響を受けません。

Cisco IOS XR ソフトウェアは、この脆弱性の影響を受けません。

Cisco NX-OS ソフトウェアは、この脆弱性の影響を受けません。

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 ASR 1000 シリーズ、Cisco ISR 4300 シリーズ、Cisco ISR 4400 シリーズ、および Cisco Cloud Services 1000v シリーズ ルータの Cisco IOS XE ソフトウェアのネットワーク アドレス変換（NAT）サービスおよびマルチプロトコル ラベル スイッチング（MPLS）サービスを必要とする IPv4 パケット処理の脆弱性により、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のリロードが引き起こされる可能性があります。

この脆弱性は、NAT と MPLS の処理を必要とする IPv4 パケットの不適切な処理に起因します。攻撃者は、NAT サービスと MPLS サービスを実行するように設定された Cisco IOS XE デバイスが処理する IPv4 パケットを送信することにより、この脆弱性を不正利用する可能性があります。攻撃者はこの不正利用により、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。

この脆弱性を不正利用するには、**ip nat inside** コマンドが設定されたインターフェイスに IPv4 パケットが到達し、**ip nat outside** コマンドと **mpls ip** コマンドが設定されたインターフェイスで送信に向けて処理される必要があります。

この脆弱性は、Cisco Bug ID CSCut96933（登録ユーザ専用）として文書化され、Common Vulnerabilities and Exposures（CVE）ID CVE-2015-6282 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。 本セキュリティ 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知ることができます。

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

またシスコでは、各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

CSCut96933 - Cisco IOS XE Software Network Address Translation Denial of Service Vulnerability 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

脆弱性の不正利用に成功すると、該当デバイスがリロードされ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, Responses, and Alerts 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、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 XE ソフトウェア

Cisco IOS XE ソフトウェアは、このアドバイザリに記載された脆弱性の影響を受けます。

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」および「 Cisco IOS XE 3S Release Notes」を参照してください。

Cisco IOS XE Software Release	First Fixed Release for this Advisory	First Fixed Release for All Advisories in the September 2015 Cisco IOS and IOS XE Software Security Advisory Bundled Publication
2.x.x	Vulnerable, migrate to 3.10.6S or later.	Vulnerable; migrate to 3.10.6S or later.
3.x.xS	Vulnerable, migrate to 3.10.6S or later.	Vulnerable; migrate to 3.10.6S or later.
3.10.xS	3.10.6S	3.10.6S
3.11.xS	Vulnerable, migrate to 3.13.3S or later.	Vulnerable; migrate to 3.13.3S or later.
3.12.xS	Vulnerable, migrate to 3.13.3S or later.	Vulnerable; migrate to 3.13.3S or later.
3.13.xS	3.13.3S	3.13.3S
3.14.xS	Vulnerable, migrate to 3.15.1S or later.	Vulnerable; migrate to 3.15.1S or later.
3.15.xS	3.15.1S	3.15.1S
3.16.xS	Not vulnerable	Not vulnerable

回避策

こ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の特有の問題をご確認ください。

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。 そのようなソフトウェア 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 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。

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 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 Navigator からソフトウェア パッチおよびバグ フィックスを入手することができます。http://www.cisco.com/cisco/software/navigator.html

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、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、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に関するお客様の状況によって異なります。 影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象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ことを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、シスコ認定パートナー、リセラー、およびディストリビュータ（認定サードパーティ ベンダー）から購入したものの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）に連絡してソフトウェア パッチおよびバグ フィックス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）
- E メール：tac@cisco.com

ソフトウェア パッチまたはバグ フィックスの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの 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 にソフトウェア パッチまたはバグ フィックスを要求してください。

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

。

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。

この脆弱性はサポート ケースの解決中に発見されました。

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 に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150923-iosxe

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 E 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
- fulldisclosure@seclists.org

本アドバイザリに関する今後の更新は 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。 更新内容については、本アドバイザリの URL でご確認ください。

今後のドキュメントや関連コンテンツの入手手順については、Security Vulnerability Policy の Receiving Security Vulnerability Information from Cisco を参照してください。

更新履歴

Revision 1.0	2015-September-23	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サポート、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の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。 この Web ページには、Cisco Security Advisory 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。

Cisco Security Advisories
Cisco Intrusion Prevention System Signatures
Cisco Applied Mitigation Bulletins
Cisco Security Blog
Cisco Event Response Pages
Cisco IntelliShield Alerts
Cisco Security Notices
Cisco Security Responses
Cisco Cyber Risk Reports
Cisco Security White Papers
Snort Rules