Cisco IOSソフトウェアのIPサービスレベル契約の脆弱性

アドバイザリーID : cisco-sa-20130327-ipsla
初公開日 : 2013-03-27 16:00
最終更新日 : 2013-04-12 14:44
バージョン 1.3 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCuc72594

CVE-2013-1148

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

IPサービスレベル契約(IP SLA)機能のCisco IOSソフトウェア実装には、IP SLAパケットの検証に脆弱性があり、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。この脆弱性に対する緩和策が用意されています。

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-20130327-ipsla

注：2013年3月27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7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3月のバンドル公開のすべての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_mar13.html

該当製品

この脆弱性は、該当するバージョンのCisco IOSソフトウェアを実行し、脆弱性のあるIP SLA汎用レスポンダ設定を持つ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、IP SLAの一般的なレスポンダ機能が設定されている場合に脆弱性の影響を受けます。

デバイスがIP SLA汎用レスポンダ用に設定されているかどうかを判断するには、次の2つの方法があります。

- デバイス設定にIP SLA general responderコマンドが含まれているかどうかを確認します。
- 実行中のデバイスでIP SLA汎用レスポンダがアクティブかどうかを確認します。

Cisco IOSデバイスでIP SLAが有効になっているかどうかを確認する推奨方法は、デバイス設定を調べて、一般的なIP SLAレスポンダが設定されているかどうかを確認することです。

デバイスの設定にIP SLA General Responderコマンドが含まれているか確認する

Cisco IOSソフトウェアの設定でIP SLA汎用レスポンダが有効になっているかどうかを確認する。ip sla responderグローバルコンフィギュレーションコマンドが存在する必要があります。show running-config | include ip sla responderコマンドを使用すると、次の例に示すように、設定にIP SLAが存在するかどうかを確認できます。

<#root>

```
Router>

show running-config | include ip sla responder$

ip sla responder
Router>
```

実行中のデバイスでIP SLA汎用レスポンダがアクティブかどうかの確認

管理者は、show ip sla responder | include ^Generalコマンドを使用します。脆弱なIP SLAの一般的なレスポンダがアクティブな場合、出力にはEnabledの行が含まれます。

次の例は、脆弱性のあるIP SLAレスポンダ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 sla responder | include ^General
General IP SLA Responder is:
Enabled
Router#
```

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

IP SLAの一般的なレスポンダ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 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

IP SLA応答側は、シスコルーティングデバイスに組み込まれたコンポーネントであり、システムがIP SLA要求パケットを予測して応答できるようにします。IP SLAレスポンダには2つのタイプがあります。

- IP SLA汎用レスポンダは、IP SLAコントロールプロトコルを使用してIP SLA動作を設定し、UDPポート1167またはUDPポート1967でパケットを受信します。
- IP SLAパーマネントレスポンダは、ユーザ設定可能なポートでUDPパケットまたはTCPパケットを受信します。

Cisco IOSソフトウェアのIP Service Level Agreement(IP SLA)general responder機能の実装における脆弱性により、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、UDPポート1167で受信されたIP SLAパケットの検証が不適切であることに起因します。攻撃者は、該当デバイス宛てに不正なIP SLA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、攻撃者は長時間のDoS状態を引き起こす可能性があります。

この脆弱性は、IPバージョン4(IPv4)またはIPバージョン6(IPv6)を介して不正利用される可能性があります。

UDPポート1967のIP SLA汎用レスポンダも、永続的なUDPレスポンダも、この脆弱性の影響を受けません。

この脆弱性は、Cisco Bug ID CSCuc72594(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-2013-1148が割り当てられています。

回避策

この脆弱性に対する回避策はありませんが、一般的なIP SLAレスポンダに導入して、インフラストラクチャアクセスリストなど、この脆弱性による影響を減らすことができる対応策があります。

IP SLAキーチェーンやコントロールプレーン保護などの従来の対応策は、この脆弱性に対する効果的な対応策ではありません。

General Responderとして設定されているデバイスの場合、ネットワーク内のCiscoデバイスに適

用可能な緩和テクニックは、
https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=27842にある付属ドキュメント『Identifying and Mitigating Exploitation of the Cisco IOS Software IP Service Level Agreement Vulnerability』で参照できます。

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 のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、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、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3月のFirst Fixed Release for All Advisories Bundled Publication列には、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されたすべての脆弱性を修正する最初の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3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3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
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-	First Fixed Release（修正され	2013年3月のバンドル公開に含まれるすべてのア

Based Releases	た最初のリリース)	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3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3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
影響を受ける 15.0 ベースのリリースはありません。		
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3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
影響を受ける 15.1 ベースのリリースはありません。		
Affected 15.2-Based Releases	First Fixed Release (修正された最初のリリース)	2013年3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
15.2GC	脆弱性なし	脆弱性あり。15.4Tの任意のリリースに移行
15.2GCA	脆弱性なし	脆弱性あり。15.4Tの任意のリリースに移行
15.2JA	脆弱性なし	15.2(2)JA
15.2JAX	脆弱性なし	脆弱性なし
15.2JB	脆弱性なし	脆弱性なし
15.2JN	脆弱性なし	脆弱性なし
1,520万	15.2(4)M3	15.2(4)M3
15.2秒	Vulnerable.脆弱性が存在するのは、リリース15.2(4)S ~ 15.2(4)S1だけです。 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)S2 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	脆弱性なし
15.2T	脆弱性なし	15.2(1)T4（2013年5月3日に入手可能） 15.2(2)T3 15.2(3)T3
Affected 15.3-Based Releases	First Fixed Release（修正された最初のリリース）	2013年3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
影響を受ける 15.3 ベースのリリースはありません。		

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す。

Cisco IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）	2013年3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
2.1.x	脆弱性なし	脆弱性なし
2.2.x	脆弱性なし	脆弱性なし
2.3.x	脆弱性なし	脆弱性なし
2.4.x	脆弱性なし	脆弱性なし
2.5.x	脆弱性なし	脆弱性なし
2.6.x	脆弱性なし	脆弱性なし
3.1.xS	脆弱性なし	脆弱性あり。3.4.5S以降に移行してください。
3.1.xSG	脆弱性なし	脆弱性なし
3.2.xS	脆弱性なし	脆弱性あり。3.4.5S以降に移行してください。
3.2xSE	脆弱性なし	脆弱性なし
3.2.xSG	脆弱性なし	脆弱性なし
3.2.XO	脆弱性なし	脆弱性なし

3.2.xSQ	脆弱性なし	脆弱性なし
3.3.xS	脆弱性なし	脆弱性あり。3.4.5S以降に移行してください。
3.3xSG	脆弱性なし	脆弱性なし
3.4.xS	脆弱性なし	脆弱性あり。3.4.5S以降に移行してください。
3.4.xSG	脆弱性なし	脆弱性なし
3.5.xS	脆弱性なし	脆弱性あり。3.7.2S以降に移行してください。
3.6.xS	脆弱性なし	脆弱性あり。3.7.2S以降に移行してください。
3.7.xS	3.7.2S	3.7.2S
3.8.xS	脆弱性なし	脆弱性なし
3.9.xS	脆弱性なし	脆弱性なし

Cisco IOS XR ソフトウェア

Cisco IOS XRソフトウェアは該当しません。

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、シスコ内部でのテストによって発見されました。

gg

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-ipsla

改訂履歴

リビジョン 1.3	2013年 4月12日	メタデータを更新するためにアドバイザリが再発行されました。アドバイザリの内容は変更されていません。
リビジョン 1.2	2013年 3月28日	「ソフトウェアバージョンと修正」セクションの修正済みソフトウェアの表を更新。
リビジョン 1.1	2013年 3月28日	「詳細」セクションを更新。
リビジョン 1.0	2013年 3月27日	初回公開リリース

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。