Cisco Security Advisory: Cisco XR 12000 Series Shared Port Adapters Interface Processor Vulnerability

Advisory ID: cisco-sa-20110525-iosxrspa

http://www.cisco.com/warp/public/707/cisco-sa-20110525-iosxrspa.shtml

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 2011 May 25 1600 UTC (GMT)

目次

要約
該当製品
詳細
脆弱性スコア詳細
影響
ソフトウェア バージョンおよび修正
回避策
修正済みソフトウェアの入手
不正利用事例と公式発表
この通知のステータス：FINAL
情報配信
更新履歴
シスコ セキュリティ手順

要約

Cisco IOS XR ソフトウェア リリース 3.9.0、3.9.1、3.9.2、4.0.0、4.0.1、4.0.2、および 4.1.0 には、認証されていないリモート ユーザが該当デバイスに特定の IP バージョン 4（IPv4）パケットを送信し、Shared Port Adapter（SPA; 共有ポート アダプタ）インターフェイス プロセッサのリロードを引き起こすことのできる脆弱性があります。

シスコはこの脆弱性に対処する無償のソフトウェア メンテナンス ユニット（SMU）をリリースしました。

これらの脆弱性に対しては回避策がありません。

このアドバイザリは次のリンクに掲載されます。 http://www.cisco.com/warp/public/707/cisco-sa-20110525-iosxrspa.shtml

該当製品

この脆弱性は、Cisco IOS XR ソフトウェア リリース 3.9.0、3.9.1、3.9.2、4.0.0、4.0.1、4.0.2、または 4.1.0 が稼動し、SPA インターフェイス プロセッサがインストールされているすべてのデバイスに影響を与えます。

脆弱性が存在する製品

この脆弱性は、Cisco XR 12000 シリーズ ルータ上の Engine 5 ラインカードすべてに影響を与えます。Engine 5 ラインカードは、SIP-600、SIP-601、SIP-501、および SIP-401 です。

シスコ製品で稼動している Cisco IOS XR 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 ライン インターフェイス (CLI) コマンドを実行してシステム バナーを表示させます。「Cisco IOS XR Software」に類似するシステム バナーによって、デバイスで Cisco IOS XR ソフトウェアが稼動していることを確認できます。ソフトウェア バージョンは「Cisco IOS XR Software」の後に表示されます。

次の例は、Cisco IOS XR ソフトウェア リリース 3.9.1 が稼動している Cisco XR 12000 シリーズ ルータを示しています。

```
RP/0/0/CPU0:example#show version
Wed Dec 15 10:16:47.117 singa

Cisco IOS XR Software, Version 3.9.1[00]
Copyright (c) 2010 by Cisco Systems, Inc.

ROM: System Bootstrap, Version 12.0(20090302:133850) [rtauro-sw30346-33S
1.23dev(0.36)] DEVELOPMENT SOFTWARE
Copyright (c) 1994-2009 by cisco Systems,  Inc.

example uptime is 26 minutes
System image file is "disk0:c12k-os-mbi-3.9.1/mbiprp-rp.vm"

cisco 12404/PRP (7457) processor with 3145728K bytes of memory.
7457 processor at 1266Mhz, Revision 1.2

1 Cisco 12000 Series Performance Route Processor
1 Cisco 12000 Series SPA Interface Processor-601/501/401
1 Cisco 12000 4 Port Gigabit Ethernet Controller (4 GigabitEthernet)
3 Management Ethernet
5 PLIM_QOS
8 FastEthernet
4 GigabitEthernet/IEEE 802.3 interface(s)
1019k bytes of non-volatile configuration memory.
982304k bytes of disk0: (Sector size 512 bytes).
62420k bytes of disk1: (Sector size 512 bytes).
65536k bytes of Flash internal SIMM (Sector size 256k).

!--- output truncated
```

デバイスに SPA インターフェイス プロセッサがインストールされているかどうかを確認するには、管理者はデバイスにログインして **show platform** コマンドを発行し、システム ラインカードを表示します。出力では、SPA インターフェイス プロセッサがインストールされていることを、「L3LC Eng 5」に似たテキストの表示によって確認できます。

次の例は、Cisco XR 12000 シリーズ ルータに Engine 5 ラインカードがインストールされている例を示しています。

```
RP/0/0/CPU0:example#show platform
Mon May  9 18:40:26.100 PST
Node            Type            PLIM            State           Config State
-------------------------------------------------------------------------------
0/0/CPU0        PRP(Active)     N/A             IOS XR RUN      PWR,NSHUT,MON
0/1/CPU0        L3LC Eng 5+     Jacket Card     IOS XR RUN      PWR,NSHUT,MON
0/1/0           SPA             SPA-8XFE-TX     READY           PWR,NSHUT
0/2/CPU0        L3LC Eng 3      GE-4            IOS XR RUN      PWR,NSHUT,MON
```

このほか、CLI コマンドの **show diag | include SPA Interface Processor** を実行することで、SPA インターフェイス プロセッサがインストールされているかどうかを表示することもできます。次の例は、デバイスに SIP-401 がインストールされている例を示しています。

```
RP/0/0/CPU0:example#show diag | include SPA Interface Processor
Mon May  9 18:44:23.069 PST
SLOT  1 (RP/LC 1): Cisco 12000 Series SPA Interface Processor- 401
RP/0/0/CPU0:example#
```

脆弱性が存在しない製品

他の Cisco IOS XR ソフトウェア リリースは、この脆弱性の影響を受けません。

次の製品または機能はこの脆弱性の影響を受けません。

- Cisco IOS ソフトウェアが稼動する Cisco 12000 シリーズ SPA インターフェイス プロセッサ
- Cisco XR 12000 シリーズの Engine 3 ラインカード
- Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ
- Cisco Carrier Routing System シリーズ ルータ

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 ファミリの 1 つである Cisco IOS XR ソフトウェアは、マイクロカーネル ベースの分散型オペレーティング システム インフラストラクチャを使用します。Cisco IOS XR ソフトウェアは、Cisco CRS、Cisco 12000 シリーズ ルータ、および Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ上で稼動します。この脆弱性は、該当する Cisco IOS XR ソフトウェアのバージョンが稼動する Cisco 12000 シリーズ ルータ上の SPA インターフェイス プロセッサにのみ影響を与えます。

Cisco IOS XR ソフトウェアの詳細については、次のリンク先で確認できます。

http://www.cisco.com/en/US/products/ps5845/index.html

この脆弱性は、該当する Cisco IOS XR ソフトウェア リリースが稼動し、SPA インターフェイス プロセッサに IPv4 アドレスが設定されているデバイスに影響を与えます。

設定されたインターフェイスのネットワーク宛て、またはネットワーク ブロードキャスト アドレス宛ての特定の IPv4 パケットを SPA インターフェイス プロセッサが受信すると、リロードが発生し、次の例に示す内容と類似したエラー メッセージを生成します。機器を通過するトラフィックは、この脆弱性のトリガーとはなりません。

```
RP/0/4/CPU0:Example#LC/0/1/CPU0:Apr 26 17:16:31.745 : tx_xbma[85]:
%L2-E5EGRESSQ-4-INTERRUPT : WIM error: reg 0x200000
```

この脆弱性は Cisco Bug ID CSCto45095 （ 登録ユーザのみ ）に文書化されており、Common Vulnerabilities and Exposures （CVE）ID として CVE-2011-1651 が割り当てられています。

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、個々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 URL にて CVSS に関する FAQ 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 計算ツールを以下の URL にて提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x

Cisco XR 12000 Series SPA Interface Processor Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Netw	Low	None	None	None	Comple

ork					te
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用に成功した場合、SPA インターフェイス プロセッサでリロードが発生する場合があります。繰り返し悪用されると、サービス拒否（DoS）状態が続く可能性があります。

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際には、 http://www.cisco.com/go/psirt/ および本アドバイザリ以降に公開のアドバイザリも参照して、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。

Major Release	**Availability of Repaired Releases**		
Affected 3.2.X through 3.8.X Based Releases	**SMU ID**	**SMU NAME**	**First Fixed Release**
	There are no affected 3.2.X through 3.8.X based releases		
Affected 3.9.X Based Releases	**SMU ID**	**SMU NAME**	**First Fixed Release**
3.9.0	None	No SMU available; Contact your Support Organization	No first fixed release; Migrate to 4.0.3, 4.1.1 or later.
3.9.1	AA04896	c12k-os-mbi-3.9.1.CSCto45095	No first fixed release; Migrate to 4.0.3, 4.1.1 or later.
3.9.2	AA0	c12k-os-mbi-	No first fixed

	4907	3.9.2.CSCto45095	release; Migrate to 4.0.3, 4.1.1 or later.
Affected 4.0.x Based Releases	**SMU ID**	**SMU NAME**	**First Fixed Release**
4.0.0	None	No SMU available; Contact your Support Organization	4.0.3
4.0.1	AA04884	c12k-4.0.1.CSCto45095	4.0.3
4.0.3	Not Affected		
Affected 4.1.x Based Releases	**SMU ID**	**SMU NAME**	**First Fixed Release**
4.1.0	AA04976	c12k-4.1.0.CSCto45095	4.1.1
4.1.1	Not Affected		

回避策

この脆弱性に対する回避策はありません。

Infrastructure Access Control List (iACL; インフラストラクチャ アクセス コントロール リスト) を使用することで、脆弱性の攻撃個所を制限できることがあります。ネットワークを通過するトラフィックを遮断することはしばしば困難ですが、インフラストラクチャ デバイスをターゲットとした許可すべきではないトラフィックを特定し、そのようなトラフィックをネットワークの境界で遮断することは可能です。iACL は、ネットワーク セキュリティのベスト プラクティスであり、長期に渡って役立つネットワーク セキュリティを付加することができます。この脆弱性で使用されるパケットのいくつかは伝送手段として UDP を使用できることから、送信元 IP アドレスが詐称される可能性があり、 信頼性のある送信元 IP アドレスからのこれらの UDP ポート宛の通信のみを許可する ACL が、回避される可能性があります。ユニキャスト RPF を、 より有効な緩和策として併用することを お勧めします。

iACL の詳細については、次のリンクの『Limit Network Access with Access Control Lists』を参照してください。 http://www.cisco.com/web/about/security/intelligence/CiscoIOSXR.html#19

修正済みソフトウェアの入手

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。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。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、または Cisco.com ダウンロード サイトの http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他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、シスコのワールドワイド Web サイト上の 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、本脆弱性に関する適切な処置について指示と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。TAC の連絡先は次のとおりです。

- +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、このお知らせの 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に対する無償アップグレードは、TAC 経由でご要求いただく必要があります。

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、 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 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、カスタマー サポート コールの処理中に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

本アドバイザリは、次のシスコのワールドワイド Web サイト上に掲載されます。

http://www.cisco.com/warp/public/707/cisco-sa-20110525-iosxrspa.shtml

ワールドワイド Web 以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- 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
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものもシスコのワールドワイド Web サイトに掲載される予定です。 しかしながら、前述のメーリング リストもしくはニュースグループに対し積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最新情報をご確認いただくことをお勧めいたします。

更新履歴

Revision 1.0	2011-May-25	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、シスコ ワールドワイド Web サイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。このページには、シスコのセキュリティ通知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。