Cisco Security Advisory: Cisco IOS Software Smart Install Remote Code Execution Vulnerability

Advisory ID: cisco-sa-20110928-smart-install

http://www.cisco.com/warp/public/707/cisco-sa-20110928-smart-install.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 1.5

Last Updated 2012 February 17 18:27 UTC (GMT)

For Public Release 2011 September 28 1600 UTC (GMT)

目次

要約

Cisco IOS ソフトウェアを実行している Cisco Catalyst スイッチのスマート インストール機能には、認証されていない攻撃者が該当デバイスに対してリモートからコードを実行できる可能性のあ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 アップデートをリリースしました。

スマート インストール機能を無効にする以外に、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に掲載されます。 http://www.cisco.com/warp/public/707/cisco-sa-20110928-smart-install.shtml

注：2011 年 9 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 10 件の Cisco Security Advisory が含まれています。9 件のアドバイザリは Cisco IOS ソフトウェアの脆弱性に対処するもので、1 件は Cisco Unified Communications Manager の脆弱性に対処するものです。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 2011 年 9 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: Semiannual 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_sep11.html

該当製品

この脆弱性の影響を受けるのは、スマート インストール機能が有効になっている Cisco Catalyst スイッチおよびシスコ サービス統合型ルータ（ISR）のみです。

脆弱性が存在する製品

スマート インストール クライアントまたはディレクタとして設定されているデバイスは、この脆弱性の影響を受けます。スマート インストール情報を表示するには、 スマート インストール ディレクタまたはクライアントで、**show vstack config** 特権 EXEC コマンドを使用します。show コマンドの出力は、ディレクタとクライアントでは異なります。次に、スマート インストール クライアントとして設定されたデバイスで **show vstack config** を使用した場合の出力を示します。

```
switch#show vstack config
 Role: Client
 Vstack Director IP address: 10.1.1.163
```

次に、スマート インストール ディレクタとして設定された Cisco Catalyst スイッチで **show vstack config** を使用した場合の出力を示します。

```
Director# show vstack config

Role: Director
 Vstack Director IP address: 10.1.1.163
 Vstack Mode: Basic
 Vstack default management vlan: 1
 Vstack management Vlans: none
 Vstack Config file: tftp://10.1.1.100/default-config.txt
 Vstack Image file: tftp://10.1.1.100/c3750e-universalk9-tar.122-
 Join Window Details:
         Window: Open (default)
         Operation Mode: auto (default)
 Vstack Backup Details:
         Mode: On (default)
         Repository: flash:/vstack (default)
```

シスコ製品で稼動している 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 ソフトウェアが稼動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_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、以下のリンクの「*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

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 IOS XE 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

スマート インストールは、新しいスイッチと Cisco ISR のゼロタッチ導入を可能にするプラグアンドプレイ構成およびイメージ管理機能です。お客様がデバイスをどこかに移動させても、ネットワークに配置して電源を入れるだけで導入でき、デバイスを設定する必要はありません。

Cisco IOS ソフトウェアを実行している Cisco Catalyst スイッチのスマート インストール機能には、認証されていない攻撃者が該当デバイスに対してリモートからコードを実行できる可能性のある脆弱性があります。スマート インストールでは、通信に TCP ポート 4786 を使用しています。この脆弱性が引き起されるのは、完全な TCP 3 ウェイ ハンドシェイク手順によって TCP 接続が確立された場合です。

この脆弱性は Cisco Bug ID CSCto10165（ 登録ユーザのみ ）に記載されており、Common Vulnerabilities and Exposures（CVE）ID CVE-2011-3271 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

CSCto10165 - Smart Install Crashes with certain IP Packets **Calculate the environmental score of**					
CVSS Base Score - **10**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **8.3**					
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、認証されていない攻撃者が該当デバイスに対してリモートからコードを実行でき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。

また、次のリンク先にある Cisco Security Intelligence Operations（SIO）ポータルで、Cisco IOS ソフトウェア チェッカーを入手できます。
http://tools.cisco.com/security/center/selectIOSVersion.x このツールでは、特定の Cisco IOS ソフトウェア バージョンに影響のあるセキュリティ アドバイザリを調べるための機能をいくつか提供しています。

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 For This Advisory」列に示されます。「First Fixed Release for All Advisories in the September 2011 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。

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2011 Bundled Publication
There are no affected 12.0 based releases		
Affected 12.1-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2011 Bundled Publication
There are no affected 12.1 based releases		
Affected 12.2-Based Relea	First Fixed Release	First Fixed Release for All Advisories in the September 2011 Bundled Publication

ses		
12.2	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2B	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2BC	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2BW	Not vulnerable	Not vulnerable
12.2BX	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2BY	Not vulnerable	Not vulnerable
12.2BZ	Not vulnerable	Not vulnerable
12.2CX	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2CY	Not vulnerable	Not vulnerable
12.2CZ	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2DA	Not vulnerable	Not vulnerable
12.2DD	Not vulnerable	Not vulnerable
12.2DX	Not vulnerable	Not vulnerable
12.2EU	Not vulnerable	Not vulnerable
12.2EW	Not vulnerable	Releases up to and including 12.2(20)EW4 are not vulnerable.
12.2EWA	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2EX	12.2(55)EX3	12.2(55)EX3
12.2EY	12.2(58)EY	12.2(58)EY
12.2EZ	Vulnerable; migrate to any release in 15.0SE Releases up to and including 12.2(53)EZ are not	Vulnerable; migrate to any release in 15.0SE

	vulnerable.	
12.2FX	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2FY	Not vulnerable	Vulnerable; First fixed in Release 12.2EX
12.2FZ	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2IRA	Not vulnerable	Vulnerable; migrate to any release in 12.2IRG
12.2IRB	Not vulnerable	Vulnerable; migrate to any release in 12.2IRG
12.2IRC	Not vulnerable	Vulnerable; migrate to any release in 12.2IRG
12.2IRD	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IRE	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IRF	Not vulnerable	Vulnerable; migrate to any release in 12.2IRG
12.2IRG	Not vulnerable	Not vulnerable
12.2IXA	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXB	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXC	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXD	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXE	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXF	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.

12.2IXG	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXH	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2JA	Not vulnerable	Not vulnerable
12.2JK	Not vulnerable	Not vulnerable
12.2MB	Not vulnerable	Not vulnerable
12.2MC	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2MRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRD
12.2MRB	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2S	Not vulnerable	Releases prior to 12.2(30)S are vulnerable; Releases 12.2(30)S and later are not vulnerable. First fixed in Release 12.2SB
12.2SB	Not vulnerable	12.2(31)SB20 12.2(33)SB10
12.2SBC	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2SCA	Not vulnerable	Vulnerable; First fixed in Release 12.2SCC
12.2SCB	Not vulnerable	Vulnerable; First fixed in Release 12.2SCC
12.2SCC	Not vulnerable	12.2(33)SCC7
12.2SCD	Not vulnerable	12.2(33)SCD6
12.2SCE	Not vulnerable	12.2(33)SCE1 12.2(33)SCE2
12.2SCF	Not vulnerable	Not vulnerable
12.2SE	Releases up to and including 12.2(50)SE5 are not vulnerable	12.2(55)SE3 12.2(58)SE

12.2SEA	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SEB	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SEC	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SED	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SEE	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SEF	Not vulnerable	Vulnerable; First fixed in Release 12.2SE
12.2SEG	Not vulnerable	Releases prior to 12.2(25)SEG4 are vulnerable; Releases 12.2(25)SEG4 and later are not vulnerable. First fixed in Release 12.2EX
12.2SG	Not vulnerable	Releases prior to 12.2(53)SG4 are vulnerable; Releases 12.2(53)SG4 and later are not vulnerable.
12.2SGA	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2SL	Not vulnerable	Not vulnerable
12.2SM	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2SO	Not vulnerable	Not vulnerable
12.2SQ	Not vulnerable	12.2(50)SQ3
12.2SRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRD
12.2SRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRD
12.2SRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRD
12.2SRD	Not vulnerable	12.2(33)SRD6
12.2SRE	Not vulnerable	12.2(33)SRE4
12.2STE	Not vulnerable	Not vulnerable
12.2S	Not vulnerable	Vulnerable; First fixed in Release

U		12.4
12.2SV	Not vulnerable	Releases prior to 12.2(29a)SV are vulnerable; Releases 12.2(29a)SV and later are not vulnerable. Migrate to any release in 12.2SVD
12.2SVA	Not vulnerable	Not vulnerable
12.2SVC	Not vulnerable	Not vulnerable
12.2SVD	Not vulnerable	Not vulnerable
12.2SVE	Not vulnerable	Not vulnerable
12.2SW	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2SX	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
12.2SXA	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
12.2SXB	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
12.2SXD	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
12.2SXE	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
12.2SXF	Not vulnerable	12.2(18)SXF17b
12.2SXH	Not vulnerable	Vulnerable; First fixed in Release 12.2SXI
12.2SXI	Not vulnerable	12.2(33)SXI6
12.2SXJ	Not vulnerable	12.2(33)SXJ1
12.2SY	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2SZ	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2T	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2TPC	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.

12.2XA	Not vulnerable	Not vulnerable
12.2XB	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2XC	Not vulnerable	Not vulnerable
12.2XD	Not vulnerable	Not vulnerable
12.2XE	Not vulnerable	Not vulnerable
12.2XF	Not vulnerable	Not vulnerable
12.2XG	Not vulnerable	Not vulnerable
12.2XH	Not vulnerable	Not vulnerable
12.2XI	Not vulnerable	Not vulnerable
12.2XJ	Not vulnerable	Not vulnerable
12.2XK	Not vulnerable	Not vulnerable
12.2XL	Not vulnerable	Not vulnerable
12.2XM	Not vulnerable	Not vulnerable
12.2XN	Not vulnerable	Not vulnerable
12.2XNA	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNB	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNC	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XND	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNE	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2X	Please see	Please see Cisco IOS-XE

NF	Cisco IOS-XE Software Availability	Software Availability
12.2XO	Not vulnerable	Releases prior to 12.2(54)XO are vulnerable; Releases 12.2(54)XO and later are not vulnerable.
12.2XQ	Not vulnerable	Not vulnerable
12.2XR	Not vulnerable	Not vulnerable
12.2XS	Not vulnerable	Not vulnerable
12.2XT	Not vulnerable	Not vulnerable
12.2XU	Not vulnerable	Not vulnerable
12.2XV	Not vulnerable	Not vulnerable
12.2XW	Not vulnerable	Not vulnerable
12.2YA	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2YB	Not vulnerable	Not vulnerable
12.2YC	Not vulnerable	Not vulnerable
12.2YD	Not vulnerable	Not vulnerable
12.2YE	Not vulnerable	Not vulnerable
12.2YF	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YG	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YH	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YJ	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2Y	Not vulnerable	Not vulnerable

K		
12.2YL	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YM	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2YN	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YO	Not vulnerable	Not vulnerable
12.2YP	Not vulnerable	Not vulnerable
12.2YQ	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YR	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YS	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YT	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YU	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YV	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YW	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YX	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YY	Not vulnerable	Vulnerable; contact your support organization per the instructions

		in the Obtaining Fixed Software section of this advisory.
12.2YZ	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2ZA	Not vulnerable	Vulnerable; First fixed in Release 12.2SXF
12.2ZB	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2ZC	Not vulnerable	Not vulnerable
12.2ZD	Not vulnerable	Not vulnerable
12.2ZE	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2ZF	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2ZG	Not vulnerable	Not vulnerable
12.2ZH	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2ZJ	Not vulnerable	Not vulnerable
12.2ZL	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2ZP	Not vulnerable	Not vulnerable
12.2ZU	Not vulnerable	Vulnerable; First fixed in Release 12.2SXH
12.2ZX	Not vulnerable	Not vulnerable
12.2ZY	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2ZYA	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2011 Bundled Publication**

There are no affected 12.3 based releases		
Affected 12.4-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2011 Bundled Publication**
There are no affected 12.4 based releases		
Affected 15.0-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2011 Bundled Publication**
There are no affected 15.0 based releases		
Affected 15.1-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2011 Bundled Publication**
15.1EY	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
15.1GC	Not vulnerable	Vulnerable; First fixed in Release 15.1T
15.1M	15.1(4)M2; Available on 30-SEP-11	15.1(4)M2; Available on 30-SEP-11
15.1MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
15.1S	Not vulnerable	15.1(2)S2 15.1(3)S
15.1T	15.1(3)T2	15.1(2)T4 15.1(1)T4 on 8-Dec-2011
15.1XB	Vulnerable; First fixed in Release 15.1T Releases up to and including 15.1(1)XB are not vulnerable.	Vulnerable; First fixed in Release 15.1T
Affected 15.2-Based	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2011 Bundled Publication**

Releases		
There are no affected 15.2 based releases		

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せん。

Cisco IOS XR ソフトウェア

Cisco IOS XR 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せん。

Cisco IOS XR ソフトウェアは、2011 年 9 月 28 日の 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

スマート インストール機能を無効にする以外に、この脆弱性を軽減する回避策はありません。クライアント スイッチでは、スマート インストール機能はデフォルトで有効になっています。クライアント スイッチで必要な設定はありません。

ネットワーク内のシスコ デバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Mitigation Bulletin』にて参照できます。
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110928-smart-install

修正済みソフトウェアの入手

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。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 Downloads 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、Digital Assurance 社の Greg Jones 氏によって発見され、シスコに報告されました。

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-20110928-smart-install.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 1.5	2012-February-17	Updated information in Cisco IOS Software table for Cisco IOS 12.2SXH

Revision 1.4	2011-December-16	Removed broken link in the Summary section
Revision 1.3	2011-October-26	Updated Cisco Bug ID information
Revision 1.2	2011-October-11	Update IOS Software table 12.2SE row
Revision 1.1	2011-September-30	Update IOS Software table bundled publication first fixed information.
Revision 1.0	2011-September-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、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。