Cisco Security Advisory: Cisco IOS Software Reverse SSH Denial of Service Vulnerability

Advisory ID: cisco-sa-20120328-ssh

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

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 ソフトウェアおよび Cisco IOS XE ソフトウェアにおけるセキュア シェル（SSH）サーバの実装には、SSH バージョン 2（SSHv2）機能にサービス拒否（DoS）の脆弱性が存在します。認証されていないリモートの攻撃者は、細工されたユーザ名で SSH リバース ログインを試行することで、この脆弱性を不正利用する可能性があります。この脆弱性の不正利用に成功した場合、攻撃者はデバイスの再起動を引き起こすことによって DoS 状態を発生させる可能性があります。繰り返し悪用されると、継続的な DoS 状態となる可能性があります。

Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの SSH サーバはオプションのサービスですが、Cisco IOS デバイスの管理におけるセキュリティのベスト プラクティスとして使用が強く推奨されています。SSHv2 接続の受け入れが設定されていないデバイスは、この脆弱性の影響を受けません。

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。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-ssh

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

該当する Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアのバージョンが稼働しているシスコ デバイスで、SSH サーバが有効にされており、かつ SSHv2 ログインが許可されている場合、この脆弱性に該当します。該当するのは SSHv2 のみです。

SSH が有効になっていることを確認するには、 **show ip ssh** コマンドを使用します。

```
  Router#show ip ssh    SSH Enabled - version 2.0    Authentication
timeout: 120 secs; Authentication retries: 3
```

上記の出力例は、SSH がこのデバイスで有効にされており、サポートされている SSH プロトコルのメジャー バージョンが 2.0 であることを示しています。Cisco IOS によって返される SSH プロトコルのバージョンの値には、次のようなものがあります。

- 1.5：SSH プロトコル バージョン 1 のみが有効
- 1.99：SSH プロトコル バージョン 1 互換の SSH プロトコル バージョン 2 が有効
- 2.0：SSH プロトコル バージョン 2 のみが有効

SSH サーバは、すべての IOS イメージに含まれているわけではありません。 **show ip ssh** コマンドが使用できない場合、そのデバイスはこの脆弱性には該当しません。 SSHv2 をサポートしていないデバイスはこの脆弱性には該当しません。

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

Cisco IOS XR 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

セキュア シェル（SSH）はネットワーク デバイスに安全なリモート アクセスを提供するプロトコルです。

Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの SSH サーバの実装には、SSH バージョン 2（SSHv2）の機能に DoS 脆弱性が存在し、認証されていないリモートの攻撃者によってデバイスが再起動させられる可能性があります。攻撃者は細工されたユーザ名で SSH リバース ログインを試行することで、この脆弱性を不正利用する可能性があります。この脆弱性の不正利用に成功した場合、攻撃者が、デバイスの再起動を引き起こすことによって DoS 状態を発生させる可能性があります。繰り返し悪用されると、継続的な DoS 状態となる可能性があります。

Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの SSH サーバはオプションのサービスですが、Cisco IOS デバイスの管理におけるセキュリティのベスト プラクティスとして使用が強く推奨されています。SSH は IOS デバイスの初期構成で AutoSecure 機能の一部として設定することができます。AutoSecure は初期構成後に実行されますが、手動で実行することも可能です。SSH は、http セキュア サーバまたはデジタル証明書のトラスト ポイントが設定されるなど、RSA キーが生成されると有効になります。SSHv2 接続の受け入れが設定されていないデバイスは、この脆弱性の影響を受けません。

この脆弱性を不正利用するには、完全な TCP 3 ウェイ ハンドシェイクが必要です。リバース SSH トラフィックは、デフォルトでは TCP ポート 22 を使用します。

この脆弱性は、Cisco Bug ID CSCtr49064 として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2012-0386 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

CSCtr49064 - Cisco IOS Software Reverse SSH Denial of Service Vulnerability 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	

影響

この脆弱性の不正利用に成功した場合、リモートの認証されていない攻撃者はデバイスの再起動を引き起こすことにより DoS 状態を発生させる可能性があります。繰り返し悪用されると、継続的な DoS 状態とな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 アーカイブや、本アドバイザリ以降に公開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性を含む場合、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）ポータルで利用できます。
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 2012 Cisco IOS Software Security Advisory Bundled Publication
There are no affected 12.0 based releases		
Affected 12.2-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the 2012 Cisco IOS Software Security Advisory Bundled Publication
12.2	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2B	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2BC	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2BW	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2BX	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2BY	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2BZ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2CX	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2CY	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2CZ	Not vulnerable	Vulnerable; First fixed in Release 12.0S
12.2DA	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2DD	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2DX	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2EU	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2EW	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2EWA	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2EX	Vulnerable; First fixed in Release 15.0SE Releases up to and including 12.2(55)EX3 are not vulnerable.	Vulnerable; First fixed in Release 15.0SE
12.2EY	12.2(58)EY2	12.2(52)EY4
12.2EZ	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2FX	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2FY	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2FZ	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2IRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE

12.2IRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRE	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRF	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRG	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2IRH	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2IXA	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2IXB	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2IXC	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2IXD	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2IXE	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2IXF	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2IXG	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2IXH	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2JA	Not vulnerable	Not vulnerable
12.2JK	Not vulnerable	Not vulnerable
12.2MB	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2MC	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2MRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2MRB	Not vulnerable	Vulnerable; contact your support organizatio the instructions in 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 12.0S
12.2SB	Not vulnerable	12.2(33)SB12
12.2SBC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SCA	Not vulnerable	Vulnerable; First fixed in Release 12.2SCE
12.2SCB	Not vulnerable	Vulnerable; First fixed in Release 12.2SCE
12.2SCC	Not vulnerable	Vulnerable; First fixed in Release 12.2SCE
12.2SCD	Not vulnerable	Vulnerable; First fixed in Release 12.2SCE
12.2SCE	Not vulnerable	12.2(33)SCE6
12.2SCF	Not vulnerable	12.2(33)SCF2

12.2SE	Vulnerable; First fixed in Release 15.0SE Releases up to and including 12.2(58)SE1 are not vulnerable.	12.2(55)SE5 *
12.2SEA	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEB	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEC	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SED	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEE	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEF	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEG	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SG	Not vulnerable	12.2(53)SG7; Available on 07-MAY-12
12.2SGA	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SL	Not vulnerable	Not vulnerable
12.2SM	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SO	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SQ	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRE	Not vulnerable	12.2(33)SRE6
12.2STE	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SU	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2SV	Not vulnerable	Releases up to and including 12.2(18)SV2 a vulnerable.
12.2SVA	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SVC	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SVD	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SVE	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SW	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.2SX	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SXA	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software

		section of this advisory.
12.2SXB	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SXD	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SXE	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SXF	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SXH	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2SXI	Not vulnerable	12.2(33)SXI9
12.2SXJ	Not vulnerable	12.2(33)SXJ2
12.2SY	Not vulnerable	12.2(50)SY2; Available on 11-JUN-12
12.2SZ	Not vulnerable	Vulnerable; First fixed in Release 12.0S
12.2T	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2TPC	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2XA	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XB	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XC	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XD	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XE	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XF	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XG	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XH	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XI	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XJ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XK	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XL	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XM	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XNA	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availabi
12.2XNB	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availabi
12.2XNC	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availabi
12.2XND	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availabi
12.2XNE	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availabi
12.2XNF	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availabi
12.2XO	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2XQ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XR	Not vulnerable	Releases prior to 12.2(15)XR are vulnerable Releases 12.2(15)XR and later are not vulnerable.First fixed in Release 15.0M
12.2XS	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XT	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XU	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XV	Not vulnerable	Vulnerable; First fixed in Release 15.0M

12.2XW	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2YA	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2YC	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2YD	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2YE	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2YK	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2YO	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2YP	Not vulnerable	Vulnerable; First fixed in Release 15.0M Releases up to and including 12.2(8)YP are vulnerable.
12.2YT	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2YW	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2YX	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2YY	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2YZ	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2ZA	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2ZB	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2ZC	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2ZD	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2ZE	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2ZH	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2ZJ	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.2ZP	Not vulnerable	Vulnerable; contact your support organizatio

		the instructions in Obtaining Fixed Software section of this advisory.
12.2ZU	Not vulnerable	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
12.2ZX	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2ZY	Not vulnerable	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
12.2ZYA	Not vulnerable	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the 2012 Cisco IOS Software Security Advisory 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 2012 Cisco IOS Software Security Advisory Bundled Publication**
12.4	Releases 12.4(13d) and prior are not vulnerable; first fixed in 12.4(25f)	Vulnerable; First fixed in Release 15.0M
12.4GC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
12.4JA	12.4(23c)JA4 12.4(25e)JA	12.4(23c)JA4 12.4(25e)JA
12.4JAX	Vulnerable; First fixed in Release 12.4JA	Vulnerable; First fixed in Release 12.4JA
12.4JDA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
12.4JDC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
12.4JDD	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
12.4JDE	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
12.4JHA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
12.4JHB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
12.4JHC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
12.4JK	Not vulnerable	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software section of this advisory.
12.4JL	Not vulnerable	Vulnerable; contact your support organizatic the instructions in Obtaining Fixed Software

		section of this advisory.
12.4JX	Vulnerable; First fixed in Release 12.4JA Releases up to and including 12.4(3g)JX2 are not vulnerable.	Vulnerable; First fixed in Release 12.4JA
12.4JY	Vulnerable; First fixed in Release 12.4JA	Vulnerable; First fixed in Release 12.4JA
12.4JZ	Vulnerable; First fixed in Release 12.4JA	Vulnerable; First fixed in Release 12.4JA
12.4MD	12.4(22)MD3; Available on 30-MAR-12	12.4(22)MD3; Available on 30-MAR-12
12.4MDA	12.4(24)MDA11	12.4(24)MDA11
12.4MDB	12.4(24)MDB5a	12.4(24)MDB5a
12.4MDC	Not vulnerable	Not vulnerable
12.4MR	Releases up to and including 12.4(16)MR1 are not vulnerable.	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.4MRA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.4MRB	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4SW	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4T	12.4(15)T16 12.4(24)T6	12.4(15)T17 12.4(24)T7
12.4XA	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XB	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XC	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XD	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XE	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XF	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XG	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XJ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XK	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XL	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.4XM	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XN	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.4XP	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.4XQ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XR	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4XT	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XV	Not vulnerable	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.4XW	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XY	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XZ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4YA	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4YB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
12.4YD	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software

	section of this advisory.	section of this advisory.
12.4YE	12.4(24)YE3d	12.4(24)YE3d
12.4YG	12.4(24)YG4	12.4(24)YG4
Affected 15.0-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.0M	15.0(1)M7	15.0(1)M8
15.0MR	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
15.0MRA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
15.0S	15.0(1)S5 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(1)S5 Cisco IOS XE devices: Please see Cisco IO Software Availability
15.0SA	Not vulnerable	Not vulnerable
15.0SE	15.0(1)SE1 15.0(2)SE; Available on 06-AUG-12	15.0(1)SE1
15.0SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability	15.0(2)SG2 Cisco IOS XE devices: Please see Cisco IO Software Availability
15.0SY	Not vulnerable	15.0(1)SY1
15.0XA	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1T
15.0XO	Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability	Cisco IOS XE devices: Please see Cisco IO Software Availability
Affected 15.1-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.1EY	15.1(2)EY1a	15.1(2)EY2
15.1GC	15.1(2)GC2	15.1(2)GC2
15.1M	15.1(4)M2	15.1(4)M4; Available on 30-MAR-12
15.1MR	15.1(1)MR3	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
15.1S	15.1(3)S2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(3)S2 Cisco IOS XE devices: Please see Cisco IO Software Availability
15.1SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Not vulnerable Cisco IOS XE devices: Please see Cisco IO Software Availability
15.1SNG	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizatio the instructions in Obtaining Fixed Software section of this advisory.
15.1SNH	Not vulnerable	Not vulnerable
15.1T	15.1(1)T4 15.1(2)T5; Available on 27-APR-12 15.1(3)T3	15.1(3)T3
15.1XB	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1T
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.2GC	15.2(1)GC1	15.2(1)GC2

15.2S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.2(1)S1 Cisco IOS XE devices: Please see Cisco IO Software Availability
15.2T	15.2(1)T2 15.2(2)T 15.2(2)T1	15.2(1)T2 15.2(2)T1 15.2(3)T; Available on 30-MAR-12

* Cisco Catalyst 3550 シリーズ スイッチは Internet Key Exchange（IKE）機能をサポートしているため、デバイスでレイヤ 3 イメージが稼働している場合、Cisco Bug ID CSCts38429 に対する脆弱性があります。ただし、この製品はソフトウェア メンテナンスが終了しています。レイヤ 2 イメージが稼働している Cisco 3550 シリーズ SMI スイッチは IKE をサポートしていないため、この脆弱性はありません。12.2SE ベースのソフトウェアが稼働している他の シスコ デバイスにも、この脆弱性はありません。

Cisco IOS XE

Cisco IOS XE

Cisco IOS XE Software Release	First Fixed Release	First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication
2.1.x	Not vulnerable	Vulnerable; migrate to 3.4.2S or later.
2.2.x	Not vulnerable	Vulnerable; migrate to 3.4.2S or later.
2.3.x	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.4.x	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.5.x	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.6.x	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
3.1.xS	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
3.2.xSG	Not vulnerable	Vulnerable; migrate to 3.2.2SG or later.
3.2.xS	Vulnerable; migrate	Vulnerable; migrate to 3.4.2S or later.

	to 3.4.2S or later.	
3.2.xSG	Not Vulnerable	3.2.2SG
3.3.xS	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
3.3.xSG	Not Vulnerable	Not Vulnerable
3.4.xS	3.4.2S	3.4.2S
3.5.xS	Not vulnerable	3.5.1S
3.6.xS	Not vulnerable	Not vulnerable

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 XR

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

IOS の SSH サーバを無効にできない場合には、一部のお客様の環境で次の回避策が役立つ場合があります。

SSH バージョン 1

この脆弱性は SSHv2 のみが影響を受けるため、ソフトウェアの更新を行うまでは、**ip ssh version 1** グローバル コンフィギュレーション コマンドを適用することで一時的に緩和することができます。この回避策を適用する前に、お客様には SSH バージョン 1 プロトコルの制限と脆弱性を確認していただく必要があります。

vty アクセス クラス

vty アクセス クラスを適用し、既知の信頼できるホストのみ SSH を介してデバイスに接続できるようにすることで、シスコ デバイスの露出を制限することができます。

vty へのトラフィック制限の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/ios/12_2/ipaddr/command/reference/1rfip1.html#wp1017389

次の例は、192.168.1.0/24 ネットブロックと 1 つの IP アドレス 172.16.1.2 からの vty ラインへのアクセスを許可し、その他からのアクセスを拒否しています。

```
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
```

シスコ プラットフォームによって、サポートするターミナル ラインの数は異なります。デバイスの構成を確認して、ご利用のプラットフォームの正確なターミナル ライン数を識別してください。

インフラストラクチャ アクセス コントロール リスト

ネットワークを通過するトラフィックをブロックするのは往々にして困難ですが、インフラストラクチャ デバイスに送られてはならないトラフィックを識別し、ネットワークの境界でそのトラフィックをブロックすることは可能です。インフラストラクチャ アクセス コントロール リスト（iACLs）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、この特定の脆弱性に対する回避策であると同時に、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。次に示す ACL の例は、インフラストラクチャ IP アドレス範囲内の IP アドレスを持つすべてのデバイスを保護するために配備されたインフラストラクチャ アクセス リストの一部として含める必要があります。

Cisco IOS が稼働するデバイスのアクセス リストの例：

```
!---
!--- SSH
access-list 150 permit tcp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK eq 22
!---   SSH
access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES MASK eq 22
!---
access-list 150 permit IP any any
interface serial 2/0
 ip access-group 150 in
```

ホワイト ペーパーの『Protecting Your Core: Infrastructure Protection Access Control Lists』は、アクセス リストによってインフラストラクチャ デバイスを保護するガイドラインと、推奨される導入方法が記載されています。このホワイト ペーパーは、次のリンクから入手可能です。
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

コントロール プレーン ポリシング

コントロール プレーン ポリシング（CoPP）機能を使用すると、これらの脆弱性を緩和できる可能性があります。次の例では、信頼できるホストが送信元であり、宛先 IP アドレスが *receive* である SSH トラフィックのみがルート プロセッサ（RP）に到達できます。

注：不明な IP アドレスや信頼できない IP アドレスからのトラフィックを廃棄するため、IP アドレスが動的に割り当てられたホストは Cisco IOS デバイスへの接続において影響を受ける可能性があります。

```
access-list 152 deny   tcp TRUSTED_ADDRESSES MASK any eq 22
access-list 152 permit tcp any any eq 22
!
class-map match-all COPP-KNOWN-UNDESIRABLE
 match access-group 152
!
!
```

```
policy-map COPP-INPUT-POLICY
 class COPP-KNOWN-UNDESIRABLE
  drop
!
control-plane
 service-policy input COPP-INPUT-POLICY
```

上の CoPP の例では、悪用パケットと一致する *permit* アクションの ACL エントリがある場合、*policy-map drop* 機能によってこれらのパケットは廃棄されますが、*deny* アクションと一致するパケットは *policy-map drop* 機能の影響を受けません。

CoPP 機能の設定と使用に関する詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

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。

この脆弱性はお客様からのお問い合わせへの対応の際に発見されました。

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-ssh

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。