# Cisco IOS and IOS XE Software SSH Version 2 RSA-Based User Authentication Bypass Vulnerability

Advisory ID: cisco-sa-20150923-sshpk

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

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 IOS ソフトウェアおよび IOS XE ソフトウェア の SSH バージョン 2（SSHv2）プロトコル実装の脆弱性により、認証されていないリモートの攻撃者がユーザ認証をバイパスできる可能性があります。

不正利用に成功すると、攻撃者はユーザの権限か、仮想テレタイプ（VTY）回線に設定された権限でログインできる可能性があります。 ユーザと VTY 回線の設定によっては、攻撃者はシステム管理者権限を取得できる可能性があります。 この脆弱性を使用して攻撃者が特権を昇格させることはできません。

攻撃者がこの脆弱性を不正利用するには、Rivest, Shamir, and Adleman（RSA）ベースのユーザ認証が設定された有効なユーザ名と、そのユーザに設定された公開キーが必要です。 この脆弱性は、公開キー認証方式（*RSA ベースのユーザ認証* とも呼ばれる機能）が設定されたデバイスにのみ影響します。

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ました。 この脆弱性に対する回避策はありません。ただし、管理者は不正利用を避けるために一時的に RSA ベースのユーザ認証を無効にすることはできます。 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-sshpk

**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

この脆弱性は、Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアの脆弱なバージョンを実行する製品に影響を与えます。 影響を受けるバージョンの詳細については、このアドバイザリの「ソフトウェア バージョンおよび修正」セクションを参照してください。

### 脆弱性が存在する製品

Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの脆弱性があるバージョンを実行するデバイスは、SSHv2 アクセスが RSA ベースのユーザ認証に設定され、1 人以上のユーザが公開キーを使用して設定されている場合に影響を受けます。

RSA ベースのユーザ認証が SSHv2 アクセスに設定されているかどうかを判断するには、**show running-config | begin ip ssh pubkey-chain** コマンドを使用して、**ip ssh pubkey-chain** コマンドが存在することと、少なくとも 1 ユーザが設定されていることを確認します。

次に、ユーザ *test-user* を認証するように設定された SSHv2 RSA ベースのユーザ認証が有効になっている Cisco IOS ルータの例を示します。

```
router#show running-config | begin ip ssh pubkey-chain
ip ssh pubkey-chain
username test-user
key-hash ssh-rsa XXXXXXXXXXXXXXXXXXXXX
[...]
```

**注**：SSHv2 RSA ベースのユーザ認証方式はデフォルトで有効になっていますが、この機能を有効にするにはユーザの公開キーを手動でインポートする必要があります。

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 デバイスが Cisco IOS ソフトウェアを実行している場合、システム バナーに「**Cisco Internetwork Operating System Software**」や「**Cisco IOS Software**」などのテキストが表示されます。 カッコ内にイメージ名が表示され、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリース名が続きます。 一部のシスコ デバイスでは、**show version** コマンドをサポートしていなかったり、別の出力が表示されたりします。

次の例は、Cisco IOS ソフトウェア リリースが 15.2(4)T1、インストールされたイメージ名が *C2951-UNIVERSALK9-M* であるシスコ製品を示しています。

```
Router> show version
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version
15.5(2)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
!--- output truncated
```

Cisco IOS ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『White Paper: Cisco IOS and NX-OS Software Reference Guide』を参照してください。

## 脆弱性が存在しない製品

Cisco IOS XRソフトウェアおよび 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 IOS SSHv2 は、キーボードインタラクティブでパスワード ベースの認証方式をサポートしています。 RSA キーの SSHv2 拡張機能は、クライアントとサーバ向けの RSA ベースの公開キー認証もサポートしています。 RSA ベースのユーザ認証では、各ユーザに関連付けられている秘密キー/公開キーのペアを認証に使用します。

Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの公開キー認証方式 SSH バージョン 2（SSHv2）実装の脆弱性により、認証されていないリモートの攻撃者がユーザ認証をバイパスできる可能性があります。

この脆弱性は、SSHv2 公開キー認証方式（Rivest, Shamir, and Adleman（RSA）ベースのユーザ認証とも呼ばれる）の実装の不備に起因します。 攻撃者は、巧妙に細工された秘密キーを使用して SSHv2 RSA ベースのユーザ認証用に設定された該当システムに認証することによって、この脆弱性を不正利用する可能性があります。 攻撃者がこの脆弱性を不正利用するには、RSA ベースのユーザ認証が設定された有効なユーザ名と、そのユーザに設定された公開キーが必要です。

不正利用に成功すると、攻撃者はユーザ認証をバイパスし、ユーザ権限または仮想テレタイプ（VTY）回線に設定された権限でログインできる可能性があります。 ユーザと VTY 回線の設定によっては、攻撃者はシステム管理者権限を取得できる可能性があります。 この脆弱性を使用して攻撃者が特権を昇格させることはできません。

この脆弱性は、Cisco Bug ID CSCus73013（ 登録ユーザ専用）として文書化され、Common Vulnerabilities and Exposures（CVE）ID CVE-2015-6280 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

| **CSCus73013 - Cisco IOS and IOS-XE SSHv2 RSA-Based User Authentication By-Pass Vulnerability Calculate the environmental score of** | | | | | |
|---|---|---|---|---|---|
| CVSS Base Score - **9.3** | | | | | |
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| Network | Medium | None | Complete | Complete | Complete |
| CVSS Temporal Score - **7.7** | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

## 影響

脆弱性の不正利用に成功した場合、攻撃者は SSHv2 RSA ベースのユーザ認証をバイパスし、ユーザ権限または VTY 回線に設定された権限でログインできる可能性があります。 ユーザと VTY 回線の設定によっては、攻撃者はシステム管理者権限を取得できる可能性があります。 この脆弱性を使用して攻撃者が特権を昇格させることはできません。

## 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 ソフトウェア

シスコでは、お客様が Cisco IOS ソフトウェアの脆弱性にさらされているかどうかを判断するためのツールを提供しています。 Cisco IOS Software Checker により、次のタスクを実行できます。

- ドロップダウン メニューからリリースを選択するか、ローカル システムからファイルをアップロードすることによって、検索を開始する
- **show version** コマンドの出力をツールで解析する
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に入れたり、特定の資料のみ、または 2015 年 9 月のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

このツールを使うことで、そのソフトウェア リリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（"First Fixed"）を特定できます。 また該当する場合、すべてのアドバイザリの脆弱性が修正された最初のリリース（"Combined First Fixed"）を特定できます。 Cisco IOS Software Checkerを参照するか、次のフィールドに Cisco IOSソフトウェア リリースを入力して、このバンドル資料のアドバイザリに該当するかどうかを判断できます。

（入力例：15.1(4)M2）

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

## Cisco IOS XE

| Cisco IOS XE Software Train | 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 |
|---|---|---|
| 2.6 | Not vulnerable | Vulnerable; migrate to 3.10.6S or later. |
| 3.1S | Not vulnerable | Vulnerable; migrate to 3.10.6S or later. |
| 3.1SG | Not vulnerable | Not vulnerable |
| 3.2S | Not vulnerable | Vulnerable; migrate to 3.10.6S or later. |
| 3.2SE | Not vulnerable | Vulnerable; migrate to 3.6.3E or later. |
| 3.2SG | Not vulnerable | Not vulnerable |
| 3.2SQ | Not vulnerable | Not vulnerable |

| | | |
|---|---|---|
| 3.2XO | Not vulnerable | Not vulnerable |
| 3.3S | Not vulnerable | Vulnerable; migrate to 3.10.6S or later. |
| 3.3SE | Not vulnerable | Vulnerable; migrate to 3.6.3E or later. |
| 3.3SG | Not vulnerable | Not vulnerable |
| 3.3SQ | Not vulnerable | Not vulnerable |
| 3.3XO | Not vulnerable | Vulnerable; migrate to 3.6.3E or later. |
| 3.4S | Not vulnerable | Vulnerable; migrate to 3.10.6S or later. |
| 3.4SG | Not vulnerable | Vulnerable; migrate to 3.6.3E or later. |
| 3.4SQ | Not vulnerable | Not vulnerable |
| 3.5E | Not vulnerable | Vulnerable; migrate to 3.6.3E or later. |
| 3.5S | Not vulnerable | Vulnerable; migrate to 3.10.6S or later. |
| 3.5SQ | Not vulnerable | Not vulnerable |
| 3.6E | 3.6.3E | 3.6.3E |
| 3.6S | Not vulnerable | Vulnerable; migrate to 3.10.6S or later. |
| 3.7E | 3.7.1E | 3.7.2E |
| 3.7S | Not vulnerable | Vulnerable; migrate to 3.10.6S or later. |
| 3.8S | Not vulnerable | Vulnerable; migrate to 3.10.6S or later. |
| 3.9S | Not vulnerable | Vulnerable; migrate to 3.10.6S or later. |
| 3.10S | 3.10.6S | 3.10.6S |
| 3.11S | 3.11.4S | Vulnerable; migrate to 3.13.3S or later. |
| 3.12S | 3.12.3S | Vulnerable; migrate to 3.13.3S or later. |
| 3.13S | 3.13.3S | 3.13.3S |
| 3.14S | 3.14.1S | Vulnerable; migrate to 3.15.1S or later. |
| 3.15S | Not vulnerable | 3.15.1S |
| 3.16S | 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。 管理者は、該当システムが脆弱性のないリリースにアップグレードされるまで一時的に SSHv2 RSA ベースのユーザ認証を無効にできます。
SSHv2 RSA ベースのユーザ認証を無効にするには、**no ip ssh server authenticate user publickey** コマンドを使用します。 この緩和策が適用されていることを確認するには、**show running-config | include ip ssh server** コマンドを使用します。

この緩和策が適用されると、システムは次の認証方式に処理を進めます。 デフォルトでは、キーボードインタラクティブになります。

次に、SSHv2 RSA ベースのユーザ認証が無効になっている Cisco IOS デバイスの例を示します。

```
Router> show version
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version
15.5(2)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
!--- output truncated
```

# 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 MiroNet AG の Mathias Seiler 氏によって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-sshpk

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