Cisco IOSソフトウェア Secure Copy（SCP）特権 拡大脆弱性

Critical

アドバイザリーID : cisco-sa-20090325-scp

初公開日 : 2009-03-25 16:00

バージョン 1.3 : Final

CVSSスコア : 9.0

回避策 : Yes

Cisco バグ ID : CSCsv38166

CVE-2009-0637

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

Cisco IOSソフトウェアの Secure Copy（SCP）実装のサーバ側は接続された Command Line Interface（CLI）ビューの認証済みユーザがどんなユーザがであるためにするために許可されるかに関係なく SCP サーバ、設定される CLI ビュー設定ごとの Cisco IOSデバイスに出入してファイルを転送することを可能にする可能性がある脆弱性が含まれています。 この脆弱性はユーザに接続される CLI ビューがそれを可能にしなくても有効 な ユーザがデバイスのファイル システムであらゆるファイルに、デバイスの保存された 設定および Cisco IOSイメージ ファイルを含んで取得するか、または書くことを可能にする可能性があります。 この設定ファイルには、パスワードなどの機密情報が含まれている場合があります。

Cisco IOS SCP サーバはデフォルトでディセーブルにされるオプションのサービスです。 CLI 意見はまたデフォルトでディセーブルにされる Cisco IOS 役割ベース CLI アクセス機能の基本的 なコンポーネントです。 Cisco IOS SCP サーバをイネーブルに設定するために明確に設定されないまたはそれを使用するために設定されるが、使用しない役割ベース CLI アクセスをデバイスはこの脆弱性から、影響を受けません。

この脆弱性は Cisco IOS SCP クライアント機能に適用しません。

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。

これらのサービスが管理者によって必要とされない場合 SCP サーバか CLI ビュー機能をディセーブルにすることから離れてこの脆弱性のために利用可能 な 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp。

注: 2009 年 3月 25 日、Cisco IOS セキュリティ アドバイザリによって組み込まれる書は 8 つのセキュリティ アドバイザリが含まれています。 アドバイザリすべては Cisco IOSソフトウェアの脆弱性に対処します。 各アドバイザリはリリースをリストしますアドバイザリの脆弱性を解決する。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS cTCP サービス拒否の脆弱性
  325-ctcp

- Cisco IOSソフトウェア倍数は IP ソケット脆弱性を特色にします
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip

- Cisco IOSソフトウェア モバイル IP およびモービル IPv6 脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip

- Cisco IOSソフトウェア Secure Copy（SCP） 特権 拡大脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp

- Cisco IOSソフトウェア Session Initiation Protocol（SIP） サービス拒否の脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip

- Cisco IOSソフトウェア複数の機能によって細工 される TCP シーケンス脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

- Cisco IOSソフトウェア複数の機能 巧妙に細工された UDP パケットの脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

- Cisco IOSソフトウェア WebVPN および SSLVPN 脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn

該当製品

修正済みソフトウェア

SCP サーバの機能性を提供するために設定され役割ベース ACL アクセスを使用するために設定される該当する Cisco IOS ソフトウェア リリースを実行する Ciscoデバイスはこの問題から影響を受けます。

脆弱 な Cisco IOS ソフトウェア リリースを実行するデバイスは設定が次に類似したである場合影響を受けています:

```
parser view <view name>
 <Definition of the CLI view>
!
username <user ID> view <view name> secret <some secret>
!
ip scp server enable
```

上のコンフィギュレーション の 断片では、**パーサー ビュー** コマンドはどんなコマンドを実行そのビューのユーザができるか規定 する意見を定義したものです。 **username コマンドは**ローカルユーザを定義し、**View キーワード**によって、ユーザに以前に定義された意見を接続します。 そして最終的に、**IP SCP サーバ enable コマンドは** Cisco IOS SCP サーバをイネーブルに設定します。

username コマンドの不在は CLI ビューの名前が認証、許可、アカウンティング（AAA）サーバによって cli ビュー**名前**アトリビュートの利用によって供給することができるのでデバイス・コンフィギュレーションがこの脆弱性から影響を受けないことを保証しません。

注: ユーザに接続される CLI ビューは AAAサーバによって供給することができます。 デバイス・コンフィギュレーションを確認するために点検することはこの脆弱性からそれ影響を受けたかどうか SCP サービスが有効に なるかどうか確認してがより適切な（**IP SCP サーバ enabled コマンド**）およびかどうかそこにである定義される CLI 意見とき（**パーサー ビュー** コマンド）。

Cisco IOS SCP サーバおよび役割ベース CLI アクセス機能はデフォルトでディセーブルにされます。

SCP サーバの機能性は暗号化可能なイメージだけで利用できます。 暗号化可能なイメージはイメージ名で "k8" か "k9" が、たとえば、"C7200-ADVSECURITYK9-M" 含まれているイメージです。 暗号化可能なイメージを実行しないデバイスは脆弱ではないです。 デバイスが暗号化可能なイメージを、**IP SCP サーバ enable コマンド**の設定の存在、CLI 意見デバイスは影響を受けていたかどうかあるかどうか（**パーサー ビュー** コマンド）の存在実行すれば、およびこれらの意見に接続したユーザが（ローカルか遠隔）確認すれば。

Cisco 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、機器にログインし 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 "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他の Cisco 機器では、 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。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih
!--- output truncated
```

次の例は C1841-ADVENTERPRISEK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 12.4(20)T を実行している Cisco製品を指定したものです:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
!--- output truncated
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide" で確認できます: http://www.cisco.com/warp/public/620/1.html。

Cisco IOS XE ソフトウェアはまたこの脆弱性から影響を受けます。

脆弱性を含んでいないことが確認された製品

Cisco IOSソフトウェアを実行しない Ciscoデバイスは影響を受けていません。

有効に なる SCP サーバ 機能を備えていないまたは機能を利用するが、ない有効に なる 役割ベース CLI 機能が Cisco IOSデバイスは影響を受けていません。

Cisco IOS XR ソフトウェアは影響を受けていません。

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。

改訂履歴

リビジョン 1.3	2009-June-26	March/09 によって結合される修正済みソフトウェア 表への取除かれた参照。
リビジョン 1.2	2009-June-1	リリース 12.4(23a) のための更新済期待された公共有効 日付。
リビジョン 1.1	2009-May-1	リリース 12.4(23a) のための更新済期待された公共有効 日付。

リビジョン 1.0	2009-March-25	初版リリース

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。