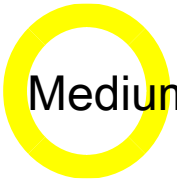
Cisco IOS Secure Copy における認可バイパスの脆弱性



アドバイザリーID : cisco-sa-20070808-scp CVE-2007-4263
初公開日 : 2007-08-08 16:00
バージョン 1.1 : Final
CVSSスコア : 6.0
回避策 : No Workarounds available
Cisco バグ ID : CSCsc19259

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 Internetwork Operating System（IOS）における Secure Copy（SCP）実装のサーバ側には、権限レベルに関係なく、すべての有効なユーザが Secure Copy サーバとして設定されている IOS デバイスとの間でファイルを送受信できる脆弱性があります。この脆弱性を利用すると、有効なユーザは、デバイスの保存済み設定などを含め、デバイスのファイルシステムに存在するすべてのファイルを取得したり書き込んだりすることができます。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。

IOS Secure Copy Server は、デフォルトでは無効になっているオプション サービスです。IOS Secure Copy Server サービスを有効にするように明示的に設定されていないデバイスは、この脆弱性には該当しません。

この脆弱性は、IOS Secure Copy Client 機能には該当しません。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-scp で公開されています。

注：2007年8月8日の公開には、4件のSecurity Advisoryと1件のSecurity Responseが含まれています。それらのアドバイザリはすべて IOS に該当し、さらに 1 つは Cisco Unified Communications にも該当します。各アドバイザリには、そのアドバイザリで説明されている脆弱性を修正したリリースが掲載されているだけでなく、4 つのアドバイザリで説明されているすべての脆弱性を修正したリリースに関する詳細も掲載されています。各ドキュメントへのリンクは次のとおりです。

- IPv6 ルーティング ヘッダー使用による Cisco IOS の情報漏えい
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-

20070808-IOS-IPv6-leak

- Cisco IOS Next Hop Resolution Protocol の脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-nhrp
- Cisco IOS Secure Copy における認可バイパスの脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-scp
- Cisco IOS および Cisco Unified Communications Manager での音声の脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-IOS-voice
- Cisco Unified MeetingPlace XSS の脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20070808-mp

該当製品

脆弱性のある製品

特定の 12.2 ベースの IOS リリースが稼働し、かつ Secure Copy サーバ機能を提供するように設定されている Cisco デバイスが、この問題に該当します。

脆弱な Cisco IOS 12.2 ベースが稼働しているデバイスでは、デバイス コンフィギュレーションに次のコマンドが存在する場合に該当します。

```
<#root>

ip scp server enable
```

IOS Secure Copy サーバはデフォルトでは無効になっています。

Secure Copy サーバ機能は、暗号化機能に対応したイメージでのみ使用できます。暗号化機能に対応したイメージ（イメージ名に k8 または k9 が含まれるイメージ）を実行していないデバイスは、脆弱ではありません。デバイスが暗号化機能に対応したイメージを実行している場合は、設定に ip scp server enable コマンドが含まれるかどうかにより、デバイスが該当するかどうかが決まります。

該当する具体的な 12.2 ベース IOS リリースについては、「ソフトウェア バージョンと修正」セクションの修正済みソフトウェアの表を参照してください。

Cisco 製品で稼働しているソフトウェアを確認するには、デバイスにログインし、show version コマンドを発行してシステム バナーを表示します。Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。出力の次の行

にカッコに囲まれたイメージ名が表示され、その後にバージョンと IOS リリース名が続きます。その他の Cisco デバイスには show version コマンドがないか、異なる出力が返されます。

IOS リリース 12.2(18)SXF10 が稼働している Cisco 製品の例を次に示します。

```
Cisco Internetwork Operating System Software
IOS (tm) s72033_rp Software (s72033_rp-IPSERVICESK9-M), Version 12.2(18)SXF10, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by cisco Systems, Inc.
Compiled Fri 13-Jul-07 08:32 by kellythw
```

Cisco IOS リリースの名前に関する詳細については、
http://www.cisco.com/warp/public/620/1.html を参照してください。

脆弱性を含んでいないことが確認された製品

IOS が稼働していない Cisco デバイスは、この脆弱性には該当しません。

Secure Copy サーバ機能が有効になっていない Cisco IOS は該当しません。

次の IOS リリース トレインは該当しません。

- 12.0 ベースのリリース
- 12.1 ベースのリリース
- 12.3 ベースのリリース
- 12.4 ベースのリリース

Cisco IOS XR は該当しません。

これらの脆弱性に該当するその他の Cisco デバイスは現在のところ見つかっていません。

詳細

Secure Copy（SCP）は Remote Copy（RCP）プロトコルに似たプロトコルであり、システム間のファイルの転送を可能にします。SCP と RCP の大きな違いは、SCP では、認証を含む転送セッションのすべての部分が暗号化された形式で実行されることであり、このために SCP の方が RCP より安全です。SCP は Secure Shell（SSH; セキュア シェル）プロトコルを利用し、デフォルトでは TCP ポート 22 を使用します。

Cisco IOS における Secure Copy 実装のサーバ側には、権限レベルに関係なく、すべての有効なユーザが Secure Copy サーバとして設定されている IOS デバイスとの間でファイルを送受信できる脆弱性があります。この脆弱性を利用すると、有効なユーザは、デバイスの保存済み設定などを含め、デバイスのファイルシステムに存在するすべてのファイルを取得したり書き込んだり

することができます。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。

この脆弱性は、認証バイパスには該当しません。ログイン クレデンシャルが検証され、有効なユーザ名とパスワードが入力された場合にのみアクセスが許可されます。この脆弱性が悪用されると、許可がバイパスされる可能性があります。

Secure Copy サーバが有効になっているデバイスは、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）が有効になっているかどうかに関係なく脆弱です。Virtual Terminal（vty; 仮想端末）経由でのログインを可能にする login コマンドにより、アクセス コントロールが vty で有効になっている場合、そのデバイスはこの脆弱性に該当します。

この脆弱性は、Cisco Bug ID CSCsc19259(登録ユーザ専用)に記載されています。

回避策

IOS Secure Copy サーバ機能が必要ない場合は、IOS Secure Copy サーバを無効にすることで、この脆弱性に対応できます。Secure Copy サーバは、グローバル コンフィギュレーション モードで次のコマンドを実行することにより無効にできます。

<#root>

```
no ip scp server enable
```

運用上の問題により Secure Copy サーバを無効にできない場合、回避策はありません。この脆弱性によるリスクは、http://www.cisco.com/JP/support/public/ht/tac/100/1008474/21-j.shtml の「Cisco ルータにおけるセキュリティの向上」で詳細に説明されているベスト プラクティスに従うことで軽減できます。この脆弱性を解決するための適切なソリューションについては、「修正済みソフトウェアの取得」のセクションを参照してください。

この属性の性質上、デバイスへのアクセスを特定の IP アドレスまたはサブネットワークに制限する Access Control List（ACL; アクセス コントロール リスト）や Control Plane Policing（CoPP; コントロール プレーン ポリシング）などのネットワークのベスト プラクティスは、有効ではない場合があります。すでに特定の IP アドレスまたはサブネットワークにアクセスを許可している場合、低い権限しか持たないユーザがデバイスとの Secure Copy セッションを確立し、この脆弱性を悪用できる可能性があります。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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機器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。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、Cisco IOS のリリース トレインが記載されています。特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（および、それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

Cisco IOSの構築、番号付け、およびメンテナンスの詳細については、次のURLを参照してください。http://www.cisco.com/warp/public/620/1.html

メジャー リリース	修正済みリリースの入手可能性	
該当する 12.0 ベースのリリース	First Fixed Release（修正された最初のリリース）	推奨リリース
該当する 12.0 ベースのリリースはありません。		
該当する 12.1 ベースのリリース	First Fixed Release（修正された最初のリリース）	推奨リリース
該当する 12.1 ベースのリリースはありません。		
該当する 12.2 ベースのリリー	First Fixed Release（修正された最初のリリース）	推奨リリース

ス		
12.2	脆弱性なし	
12.2B	脆弱性なし	
12.2BC	脆弱性なし	
12.2BW	脆弱性なし	
12.2BY	脆弱性なし	
12.2BZ	脆弱性なし	
12.2CX	脆弱性なし	
12.2CY	脆弱性なし	
12.2CZ	脆弱性なし	
12.2DA	脆弱性なし	
12.2DD	脆弱性なし	
12.2DX	脆弱性なし	
12.2EU	脆弱性なし	
12.2EW	脆弱性なし	

12.2EWA	脆弱性なし	
12.2EX	脆弱性なし	
12.2EY	脆弱性なし	
12.2EZ	脆弱性なし	
12.2FX	脆弱性なし	
12.2FY	脆弱性なし	
12.2FZ	脆弱性なし	
12.2IXA	脆弱性あり(最初の修正は 12.2(18)IXD1)	12.2(18)IXD1
12.2IXB	脆弱性あり(最初の修正は 12.2(18)IXD1)	12.2(18)IXD1
12.2IXC	脆弱性あり(最初の修正は 12.2(18)IXD1)	12.2(18)IXD1
12.2IXD	12.2(18)IXD1	12.2(18)IXD1
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	

12.2MB	脆弱性なし	
12.2MC	脆弱性なし	
12.2S	脆弱性なし	
12.2SB	脆弱性なし	
12.2SBC	脆弱性なし	
12.2SE	脆弱性なし	
12.2SEA	脆弱性なし	
12.2SEB	脆弱性なし	
12.2SEC	脆弱性なし	
12.2SED	脆弱性なし	
12.2SEE	脆弱性なし	
12.2SEF	脆弱性なし	
12.2SEG	脆弱性なし	
12.2SG	脆弱性なし	
12.2SGA	脆弱性なし	

12.2SL	脆弱性なし	
12.2SM	脆弱性なし	
12.2SO	脆弱性なし	
12.2SRA	脆弱性なし	
12.2SRB	脆弱性なし	
12.2SU	脆弱性なし	
12.2SV	脆弱性なし	
12.2SVA	脆弱性なし	
12.2SVC	脆弱性なし	
12.2SW	脆弱性なし	
12.2SX	脆弱性なし	
12.2SXA	脆弱性なし	
12.2SXB	脆弱性なし	
12.2SXD	脆弱性あり。TACに連絡	
12.2SXE	脆弱性あり(最初の修正は	12.2(18)SXF10

	12.2(18)SXF9)	
12.2SXF	12.2(18)SXF9	12.2(18)SXF10
12.2SXH	脆弱性なし	
12.2SY	脆弱性なし	
12.2SZ	脆弱性なし	
12.2T	脆弱性なし	
12.2TPC	脆弱性なし	
12.2UZ	脆弱性なし	
12.2VZ	脆弱性なし	
12.2XA	脆弱性なし	
12.2XB	脆弱性なし	
12.2XC	脆弱性なし	
12.2XD	脆弱性なし	
12.2XE	脆弱性なし	
12.2XF	脆弱性なし	

12.2XG	脆弱性なし	
12.2XH	脆弱性なし	
12.2XI	脆弱性なし	
12.2XJ	脆弱性なし	
12.2XK	脆弱性なし	
12.2XL	脆弱性なし	
12.2XM	脆弱性なし	
12.2XN	脆弱性なし	
12.2XQ	脆弱性なし	
12.2XR	脆弱性なし	
12.2XS	脆弱性なし	
12.2XT	脆弱性なし	
12.2XU	脆弱性なし	
12.2XV	脆弱性なし	
12.2XW	脆弱性なし	

12.2YA	脆弱性なし	
12.2YB	脆弱性なし	
12.2YC	脆弱性なし	
12.2YD	脆弱性なし	
12.2YE	脆弱性なし	
12.2YF	脆弱性なし	
12.2YG	脆弱性なし	
12.2YH	脆弱性なし	
12.2YJ	脆弱性なし	
12.2YK	脆弱性なし	
12.2YL	脆弱性なし	
12.2YM	脆弱性なし	
12.2YN	脆弱性なし	
12.2YO	脆弱性なし	
12.2YP	脆弱性なし	

12.2YQ	脆弱性なし	
12.2YR	脆弱性なし	
12.2YS	脆弱性なし	
12.2YT	脆弱性なし	
12.2YU	脆弱性なし	
12.2YV	脆弱性なし	
12.2YW	脆弱性なし	
12.2YX	脆弱性なし	
12.2YY	脆弱性なし	
12.2YZ	脆弱性なし	
12.2ZA	脆弱性なし	
12.2ZB	脆弱性なし	
12.2ZC	脆弱性なし	
12.2ZD	脆弱性なし	
12.2ZE	脆弱性なし	

12.2ZF	脆弱性なし	
12.2ZG	脆弱性なし	
12.2ZH	脆弱性なし	
12.2ZJ	脆弱性なし	
12.2ZL	脆弱性なし	
12.2ZP	脆弱性なし	
12.2ZR	脆弱性なし	
12.2ZU	脆弱性あり。最初の修正は 12.2(33)SXHで、2007年8月31日に入手可能	12.2(33)SXH（2007年 8 月 31 日に入手可能）
12.2ZW	脆弱性なし	
12.2ZY	脆弱性なし	
該当する 12.3 ベースのリリース	First Fixed Release（修正された最初のリリース）	推奨リリース
該当する 12.3 ベースのリリースはありません。		
該当する	First Fixed	推奨リリース

12.4 ベースのリリース	Release（修正された最初のリリース）	
該当する 12.4 ベースのリリースはありません。		

推奨事項

$propertyAndFields.get("recommendations")

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やその公表は確認しておりません。

この脆弱性は、University of North Carolina at Greensboro の Vijay Sarvepalli から Cisco に報告されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-scp

改訂履歴

リビジョン 1.0	2007 年 8 月 8 日	初版リリース

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。