IOS FTP サーバの複数の脆弱性

Critical

アドバイザリーID : cisco-sa-20070509-iosftp

初公開日 : 2007-05-09 16:00

バージョン 1.4 : Final

CVSSスコア : 10.0

回避策 : No Workarounds available

Cisco バグ ID : CSCsg16908

CVE-2007-2586

CVE-2007-2587

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 FTP サーバ機能には複数の脆弱性があり、これらを悪用すると、サービス拒否（DoS）状態、ユーザ クレデンシャルの不適切な検証、およびデバイスに関する保存済み設定を含むデバイス ファイルシステムからの任意のファイルの取得または書き込みなどが発生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。

IOS FTP サーバは、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 FTP サーバサービスを有効にするよう特に設定されていないデバイスは、これらの脆弱性には該当しません。

この脆弱性は、IOS FTP クライアント機能には該当しません。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070509-iosftp で掲示されます。

該当製品

脆弱性のある製品

IOS が稼働していて、FTP サーバ機能が設定されている Cisco デバイスが、これらの脆弱性に該当します。

11.3、12.0、12.1、12.2、12.3、および 12.4 に基づく IOS バージョンには、IOS FTP サーバ機能が組み込まれています。 IOS FTP サーバ機能は、CSCsg16908 で削除されています。

前述の IOS トレインに基づく特定の IOS リリースにのみ、IOS FTP サーバ機能が組み込まれています。 Cisco IOS が稼働しているデバイスのうち、この脆弱性に該当するのは、次のコマンドをデバイス設定に含んでいるデバイスだけです。

```
ftp-server enable
```

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。

FTP サーバ機能が有効になっていない Cisco IOS デバイスは該当しません。

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

IOS FTP サーバ機能には、複数の脆弱性があります。 これらの脆弱性は、次の Cisco Bug ID に記述されています。

- CSCek55259：Improper authorization checking in IOS FTP server
- CSCse29244：IOS reload when transferring files via FTP

IOS の FTP サーバにはこのような問題があるため、この機能は削除されています。 Cisco では、完全な機能を提供する安全な FTP サーバ機能を将来的に追加することを検討しています。

IOS FTP サーバ機能の削除に関しては、Cisco Bug ID CSCsg16908 で取り扱われています。

脆弱性スコア評価の詳細

Cisco では、Common Vulnerability Scoring System（CVSS）に基づき、このアドバイザリで説明されている脆弱性のスコアを評価しました。

Cisco では基本スコアと現状スコアを評価します。 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。

Cisco PSIRT は、すべてのケースにおける重みを「標準」に設定します。 特定の脆弱性の環境的影響を判断する際には、重みパラメータを適用することを推奨します。

CVSS は、脆弱性の重大度を伝える標準ベースのスコア評価方式であり、対応の緊急度や優先度

を判断するのに役立ちます。

Cisco は http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html で CVSS に関する追加質問に答えるために FAQ を提供しました。

Cisco はまた http://tools.cisco.com/security/center/cvssCalculator.x で個々 の ネットワークのための環境影響の計算を助けるように CVSS カルキュレータを提供しました。

CSCek55259：Improper authorization checking in IOS FTP **CSCek55259 の環境スコアを計算する**						
CVSS 基本スコア：**10**						
攻撃元区分	攻撃条件の複雑さ	認証	機密性への影響	完全性への影響	可用性への影響	影響の重み
Remote	低	不要	Complete	Complete	Complete	Normal
CVSS 現状スコア：**8.3**						
攻撃される可能性		利用可能な対策のレベル		Report Confidence		
機能する		Official-Fix		確認済		

CSCse29244：IOS reload when transferring files via FTP **CSCse29244 の環境スコアを計算する**						
CVSS 基本スコア：**2.0**						
攻撃元区分	攻撃条件の複雑さ	認証	機密性への影響	完全性への影響	可用性への影響	影響の重み
Remote	低	必要	なし	なし	Complete	Normal
CVSS 現状スコア：**1.7**						
攻撃される可能性		利用可能な対策のレベル		Report Confidence		
機能する		Official-Fix		確認済		

回避策

次のコマンドをコンフィギュレーション モードで実行することにより、IOS FTP サーバ機能の使用を無効にできます。

```
no ftp-server enable
```

Cisco 機器に適用可能な追加の軽減策については以下の "Cisco Applied Intelligence companion document" より入手可能です。

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070509-iosftp

代替ファイル転送メカニズム

Cisco IOS は、デバイスでのファイル転送に関して複数の方式をサポートしています。 そのうちの 1 つが、Secure Copy（SCP）です。 SCP は、強力な暗号化をサポートする Cisco IOS イメージでサポートされています。 SCP の機能についての詳細は、次の URL で確認できます。

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t2/feature/guide/ftscp.html

この他に、IOS の Trivial File Transfer Protocol（TFTP）サーバを使用する方法もあります。 TFTP サーバの設定については、次のリンク先を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf011_ps1835_TSD_Products_Configuration_Guide_Chapter.html

IOS の FTP サーバを無効にできない場合には、次のいずれかのメカニズムを使用してデバイスへの FTP アクセスを制限できます。

インフラストラクチャ ACL（iACL）

ネットワークを移動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 ACL はネットワーク セキュリティのベスト プラクティスと考えられており、ここでの特定の脆弱性の回避策としてだけでなく、優れたネットワーク セキュリティへの長期的な付加機能として考慮する必要があります。 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：

```
no ftp-server enable
```

ホワイトペーパー 『Protecting Your Core: Infrastructure Protection Access Control Lists (ACL) には、インフラストラクチャ保護アクセス リストに関するガイドラインと推奨配備方法が記載されています。 この White Paper は次のサイトで提供されています。 http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml 。

レシーブ ACL（rACL）

分散型のプラットフォームにおいては、Cisco12000 シリーズ(GSR) では 12.0(21)S2、Cisco7500 シリーズでは 12.0(24)S、Cisco10720 シリーズでは 12.0(31)S の IOS ソフトウェアにてサポートされている Receive ACL も選択肢となります。 受信 ACL は、ルート プロセッサが有害なトラフィックの影響を受ける前に、そのトラフィックからデバイスを保護します。 受信 ACL は、それが設定されたデバイスのみを保護する設計になっています。 Cisco 12000, 7500, 10720 では通過トラフィックは Receive ACL による影響を受けません。 このため、以下の ACL の例において宛先 IP アドレス "any" が用いられても、自ルータの物理あるいは仮想 IP アドレスのみが参照されます。 受信 ACL はネットワーク セキュリティのベスト プラクティスと考えられており、ここでの特定の脆弱性の回避策としてだけでなく、優れたネットワーク セキュリティへの長期的な付加機能として考慮する必要があります。 ホワイトペーパーGSR 受信アクセス コントロール リスト』は、正当なトラフィックを識別してデバイスに許可を与え、望ましくないパケットをすべて拒否するのに役立ちます。
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml
。

次の receive path ACL は信頼できるホストからのこのようなタイプのトラフィックを許可するように記述されています。

```
no ftp-server enable
```

コントロール プレーン ポリシング（CoPP）

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 FTP 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。

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ことにより、Cisco IOS デバイスへの接続で IP アドレスが動的に割り当てられたホストには影響が及ぶ可能性がある点に注意してください。

```
no ftp-server enable
```

上の CoPP の例では、「permit」アクションがあり悪用パケットと一致する ACL エントリがある場合、ポリシー マップの「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ポリシー マップ drop 機能の影響を受けません。

CoPP は、Cisco IOS リリース トレイン 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T で使用できます。

CoPP 機能の設定と使用方法についての詳細は、次の URL で確認できます。

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

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 およびそれ以降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、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（「第 1 修正済みリリース」）とそれぞれの提供日が「リビルド」列と「メンテナンス」列に記載されます。 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。 このようなリリースは、少なくとも、示されているリリース以上（最初の修正リリース ラベル以上）にアップグレードしてする必要があります。

下の表に記載されていないソフトウェア リリースは該当しません。

「リビルド」および「メンテナンス」という用語の詳細は、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	**リビルド**	**メンテナンス**
12.0	脆弱性あり; 12.2(40a) またはそれ以降への移行する	
12.0T	脆弱性あり; 12.2(40a) またはそれ以降への移行する	
12.0XC	脆弱性あり; 12.2(40a) またはそれ以降への移行する	
12.0XK	脆弱性あり; 12.2(40a) またはそれ以降への移行する	
12.0WC	12.0(5)WC17	
該当する 12.1 ベースのリリース	**リビルド**	**メンテナンス**
12.1	脆弱性あり; 12.2(40a) またはそれ以降への移行する	
12.1T	脆弱性あり; 12.2(40a) またはそれ以降への移行する	

12.1XH	脆弱性あり; 12.2(40a) またはそれ以降への移行する	
12.1XM	脆弱性あり; 12.3(21)or 以降への移行する	
該当する 12.2 ベースのリリース	**リビルド**	**メンテナンス**
12.2	12.2(40a)	12.2(46)
12.2T	脆弱性あり; 12.3(21) またはそれ以降への移行する	
12.2XA	脆弱性あり; 12.3(21) またはそれ以降への移行する	
12.2XG	脆弱性あり; 12.3(21) またはそれ以降への移行する	
12.2XT	脆弱性あり; 12.3(21) またはそれ以降への移行する	
12.2ZF	脆弱性あり; 12.4(12) またはそれ以降への移行する	
12.2ZH	脆弱性あり; contact TAC	
12.2ZJ	脆弱性あり; 12.4(12) またはそれ以降への移行する	
12.2ZL	脆弱性あり; contact TAC	
12.2ZN	脆弱性あり; 12.4(12) またはそれ以降への移行する	
該当する 12.3 ベースのリリース	**リビルド**	**メンテナンス**
12.3		12.3(21)
12.3B	脆弱性あり; 12.4(12) またはそれ以降への移行する	
12.3T	脆弱性あり; 12.4(12) またはそれ以降への移行する	
12.3TPC	脆弱性あり; contact TAC	
12.3XA	脆弱性あり; contact TAC	
12.3XC	脆弱性あり; contact TAC	
12.3XD	脆弱性あり; 12.4(12) またはそれ以降への移行する	
12.3XE	脆弱性あり; contact TAC	
12.3XF	脆弱性あり; 12.4(12) またはそれ以降への移行する	
12.3XG	脆弱性あり; contact TAC	
12.3XH	脆弱性あり; 12.4(12) またはそれ以降への移行する	
12.3XK	脆弱性あり; 12.4(12) またはそれ以降への移行する	
12.3XQ	脆弱性あり; 12.4(12) またはそれ以降への移行する	
12.3XR	脆弱性あり; contact TAC	

12.3XS	脆弱性あり; 12.4(12) またはそれ以降への移行する	
12.3XX	12.3(8)XX2d	
12.3YA	脆弱性あり; 12.4(12) またはそれ以降への移行する	
12.3YD	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YG	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YH	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YI	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YK	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YM	脆弱性あり; contact TAC	
12.3YS	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YT	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YZ	脆弱性あり; contact TAC	
該当する 12.4 ベースのリリース	**リビルド**	**メンテナンス**
12.4	12.4(10b)	
	12.4(3g)	
	12.4(7d)	
	12.4(8c)	12.4(12)
12.4SW	脆弱性あり; contact TAC	
12.4T	12.4(4)T6	
	12.4(6)T6	
	12.4(9)T2	12.4(11)T
12.4XA	脆弱性あり; 12.4(6)T6 またはそれ以降への移行する	
12.4XC	12.4(4)XC6	
12.4XD	12.4(4)XD4	
12.4XE	12.4(6)XE2	

不正利用事例と公式発表

2008 年の 12 月では、Phenoelit の FX は無秩序通信議会によって資格を与えられた「Cisco IOS 攻撃でプレゼンテーションを提供し、彼が彼をアサートしたかどれの間に防御は」、この脆弱性を利用するエクスプロイトを案出しました。 新しい脆弱性は 2008 年の無秩序通信議会の FX のプレゼンテーションの間に表われませんでした。

http://events.ccc.de/congress/2008/Fahrplan/events/2816.en.html

Cisco はこの脆弱性のあらゆる悪質な宣伝に気づいていません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070509-iosftp

改訂履歴

リビジョン 1.4	2009-January-09	不正利用事例と公式発表 セクションを DEC 2008 無秩序通信会議で学ばれた情報を示すためにアップデートしました。
リビジョン 1.3	2008-May-14	回避策 > レシーブ ACL セクションへの更新。
リビジョン 1.2	2008-April-25	CSCek55259 および CSCse29244 のために記録する CVSS への更新済リンク。
リビジョン 1.1	2007 年 5 月 9 日	軽微な文法上とスタイル上の編集
リビジョン 1.0	2007 年 5 月 9 日	初版リリース

利用規約