Cisco IOS DHCP によってブロックされるインターフェイス サービス拒否

severity	**アドバイザリーID :** cisco-sa-20041110-dhcp	CVE-2004-1111
	初公開日 : 2004-11-10 17:00	
	バージョン 1.2 : Final	
	回避策 : Yes	
	Cisco バグ ID :	

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

有効に なる ダイナミック ホスト コンフィギュレーション プロトコル サーバかリレー エージェントがある Cisco IOSバージョン 12.2S のブランチを実行する Cisco IOSÂ® デバイスは設定されなくて、とりわけ巧妙に細工された DHCP パケットを受信するときインプットキューがブロックされるようになるサービス拒否に脆弱でも。 Cisco はこの問題に対処するために自由な修正済みソフトウェアを提供しています。 またこの脆弱性を軽減する回避策があります。 この問題は CSCdx46180 に含まれていた修正によってもたらされ、Cisco バグ ID CSCee50294 （登録ユーザのみ）によってトラッキングされています。

このアドバイザリは 110-dhcp で利用できます。

該当製品

修正済みソフトウェア

Cisco IOSバージョン 12.2(14)SZ を実行する以下のシスコ製品か Cisco IOS 12.2(18)S のバリアントはこの脆弱性から（次のセクションでリストされているように）およびより高く影響を受けます。

- Cisco 7200、7300、7500 のプラットフォーム
- Cisco 2650、2651、2650XM、2651XM マルチサービスプラットフォーム
- Cisco ONS15530、ONS15540
- Cisco Catalyst 4000、Sup2plus、Sup3、Sup4 および Sup5 モジュール
- Cisco Catalyst 4500、Sup2Plus TS
- Cisco Catalyst 4948、2970、3560、および 3750

- Cisco Catalyst 6000、Sup2/MSFC2 および Sup720/MSFC3
- Cisco 7600 Sup2/MSFC2 および Sup720/MSFC3

この問題は設定コマンド **no service dhcp** がない影響を受けた Cisco IOSバージョン 12.2(18)EW、12.2(18)EWA、12.2(14)SZ、12.2(18)S、12.2(18)SE、12.2(18)SV、12.2(18)SW およびより高いを実行する Ciscoデバイスだけ影響を与えます。 それはこの脆弱性はのために設定されるべき DHCPサーバかリレー エージェントに必要です提供および不正利用されてではないです;「service dhcp」は IOS でデフォルトで有効に なり、この脆弱性の不正利用に（インターフェイス アドレスに加えて）必要な唯一の設定です。 これには Cisco IOSソフトウェアを実行するルータが、またスイッチおよびラインカード含まれています。 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 コマンド **no service dhcp** と影響を受けた Cisco IOSソフトウェアを実行する Ciscoデバイスは影響を受けていません。

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「インターネットワーク オペレーティング システム ソフトウェア」として識別しますそれ自身をまたは単に「IOSÂ®」。 出力次の行で、イメージ名は「バージョンに」先行しているかっこ IOSリリース名の間で表示する。 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。

次の例は C2500-IS-L のインストール済みイメージ名前と IOS リリース 12.0(3) を実行する Cisco製品を指定したものです:

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

リリース トレイン ラベルは "12.0." です

次 の 例は C2600-JS-MZ のイメージ名と Cisco IOS Release 12.0(2a)T1 を実行する製品を示します:

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

Cisco IOS リリース指名についてのその他の情報は http://www.cisco.com/warp/public/620/1.html で見つけることができます。

脆弱性を含んでいないことが確認された製品

有効に なる コマンド **no service dhcp** と影響を受けた Cisco IOSソフトウェアを実行する Ciscoデバイスは影響を受けていません。

ソフトウェア バージョン および 修正 下記の表にリストされていない IOSバージョンを実行するシスコ製品は影響を受けていません。

Cisco IOSソフトウェアを実行しないし、この脆弱性から含んでいる影響を受けないシスコ製

品は、に制限されませんが:

- 700 シリーズ ダイヤルアップルータ（750、760、および 770 シリーズ）は影響を受けていません。
- IGX、BPX および MGX 行のような WANスイッチングプロダクトは影響を受けていません。
- ホストベース ソフトウェアは影響を受けていません。
- Cisco PIX Firewall は影響を受けていません
- Cisco LocalDirector は影響を受けていません。
- Cisco Content Engine および ACNS は影響を受けていません。
- CatOS が稼働している Catalyst 2901/2902、2948G、2980G、4000、5000、および 6000 のスイッチ。
- Cisco Network Registrar は影響を受けていません。
- Cisco VPN 3000 シリーズは影響を受けていません
- Cisco IOS XR プラットフォームは影響を受けていません。
- Cisco MDS 9000 ファミリーは影響を受けていません。

改訂履歴

リビジョン 1.2	2004-December-1	更新済ソフトウェア バージョン 表- 12.2(20)EW.
リビジョン 1.1	2004-November-10	Workaround セクションへの追加されたネットワーク リビュー免責事項テキスト。
リビジョン 1.0	2004-November-10	初回公開リリース

利用規約