

NTPの脆弱性



アドバイザリーID : cisco-sa-20020508-ntp- [CVE-2001-0414](#)
vulnerability

初公開日 : 2002-05-08 16:00

バージョン 2.1 : Final

回避策 : No Workarounds available

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

ネットワークタイムプロトコル(NTP)は、複数のデバイスで時刻を同期するために使用されます。NTPデーモンクエリ処理機能に脆弱性が発見されました。この脆弱性は公開されています。

次の製品は、この脆弱性の影響を受けることが確認されています。

- Cisco IOSソフトウェアのすべてのリリース
- Media Gateway Controller (MGC) および関連製品
- BTS10200
- Cisco IPマネージャ

その他のシスコソフトウェアアプリケーションはSolarisプラットフォーム上で動作する場合があります。これらの製品が特定されていない場合は、通常のメンテナンス手順に従ってセキュリティパッチを定期的にインストールする必要があります。

シスコでは、影響を受ける可能性のある他の製品についてこの問題の調査を継続しています。特に明記されていない限り、他のすべての製品は影響を受けないと見なされます。

この影響を緩和するには、[回避策](#)があります。

このアドバイザリーは、

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020508-ntp-vulnerability>で確認できます。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

次の製品が影響を受けます。

- Cisco IOSソフトウェアのすべてのリリース
- メディアゲートウェイコントローラ(MGC)および関連製品には、次の製品が含まれます。
 - SC2200
 - Cisco仮想スイッチコントローラ(VSC3000)
 - Cisco PGW2200公衆電話交換網(PSTN)ゲートウェイ
 - Cisco Billing and Management Server(BAMS)
 - Cisco Voice Services Provisioning Tool(VSPT)
- BTS10200
- Cisco IPマネージャ

その他のシスコソフトウェアアプリケーションはSolarisプラットフォーム上で動作する場合があります。これらの製品が特定されていない場合は、通常のメンテナンス手順に従ってセキュリティパッチを定期的にインストールする必要があります。

脆弱性を含んでいないことが確認された製品

次の製品は影響を受けません。

- IP専用イメージを実行するCiscoルータ1600/1600-R
- Ciscoルータ801、803、811、813、1003
- Cisco Content Service Switch 11000シリーズ
- Cisco Secure PIXファイアウォール
- Catalyst 6000ファミリスイッチ (すべてのCatOSリリース)
- Catalyst 5000ファミリスイッチ、すべてのCatOSリリース
- Catalyst 4000ファミリスイッチ、すべてのCatOSリリース

シスコでは、影響を受ける可能性のある他の製品についてこの問題の調査を継続しています。特に明記されていない限り、他のすべての製品は影響を受けないと見なされます。

詳細

巧妙に細工されたNTP制御パケットを送信することにより、NTPデーモンでバッファオーバーフローを引き起こす可能性があります。この脆弱性は、リモートから悪用される可能性があります。不正利用に成功すると、ターゲットマシンで任意のコードが実行される可能性があります。このような不正利用が可能な場合は、かなりのエンジニアリングスキルと、Cisco IOSソフトウェアまたはSUN Solarisオペレーティングシステムの内部動作に関する完全な知識が必要になります。

この脆弱性は、デバイスが果たす役割に関係なく存在します。デバイスがNTPサーバまたはクライアントである場合でも、脆弱性が存在します。

IOSについては、この脆弱性はCisco Bug ID CSCdt93866およびCSCdw35704に記載されています。

NTPソフトウェアのメインリポジトリとNTPに関するその他すべての情報は、<http://www.ntp.org/>で確認できます。

回避策

このセクションでは、回避策について説明します。

Cisco IOS

曝露を軽減する方法は複数ある。これらの方法を組み合わせることも、個別に使用することもできます。

- IOSによるNTPクエリの処理を一切禁止します。サーバまたはクライアントのどちらとして動作しているかによって、設定が異なります。次に、各設定について説明します。
サーバとしてのみ動作し、他のユーザによって同期されない場合は、次の設定を使用できます。

```
ntp access-group serve-only 20  
  
access-list 20 permit any
```

上記の設定では、すべてのピアがNTP要求を送信できます。必要に応じて、許可するクライアントを制限できます。この場合、次の例のように、ACL 20を変更して正規のクライアントだけを含めることができます

```
ntp access-group serve-only 20  
access-list 20 permit <ntp client #1>  
access-list 20 permit <ntp client #2>
```

クライアントとしてのみ動作する場合は、次の設定を使用できます。

```
ntp server <ntp server #1>  
ntp server <ntp server #2>  
ntp access-group peer 10  
access-list 10 permit host <ntp server #1>  
access-list 10 permit host <ntp server #2>
```

上記の設定では、このデバイスをいずれかのサーバで同期できます。これは制御パケットの実行を妨げないため、公開を制限するだけであることに注意してください。ただし、サーバから送信された制御パケットだけが処理されます。

サーバおよびクライアントとして機能する場合は、次の設定を使用できます。

```
ntp server <ntp server #1>
ntp server <ntp server #2>
ntp access-group peer 10
ntp access-group serve-only 20
access-list 10 permit host <ntp server #1>
access-list 10 permit host <ntp server #2>
access-list 20 permit <ntp client #1>
access-list 20 permit <ntp client #2>
```

上記の設定により、ルータは任意のNTP要求に応答でき、特定のサーバによって同期できるようになります。これは制御パケットの実行を妨げないため、公開を制限するだけであることに注意してください。ただし、サーバから送信された制御パケットだけが処理されます。

- ACLを使用して、正当なサーバからのものではないすべてのNTPパケットをドロップすることで、問題の発生を軽減できます。これは次のように実行できます。

```
access-list 10 permit <ntp server #1>
access-list 10 permit <ntp server #2>
access-list 10 deny any
!
ntp access-group peer 10
```

上記の例では、<ntp server #1>および<ntp server #2>は、NTPパケットが受け入れられるピアまたはサーバのアドレスです。

- また、ネットワークの外部のNTPサーバを使用していない場合は、ネットワーク境界ですべてのNTPパケットをドロップできます。これは、次の行を既存のACLに統合することで実行できます

```
access-list 101 deny udp any any eq ntp
```

既存のACLがない場合は、次のACLをネットワーク境界で使用して、ntpだけを拒否し、残りのIPトラフィックを許可できます

```
access-list 101 deny udp any any eq ntp
access-list 101 permit ip any any
```

個々のコマンドとその他の例の詳細については、次の文書を参照してください。

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd303.htm

- <http://www.cisco.com/public/cons/isp/essentials/>

MGCおよび関連製品

Cisco IPマネージャ

BTS10200

回避策はBugtraqリストに掲載されていますが、提供されたパッチをインストールすることをお勧めします。

ユーザは、パッチの一部であるインストール手順に従う必要があります。

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わせください。

MGCおよび関連製品

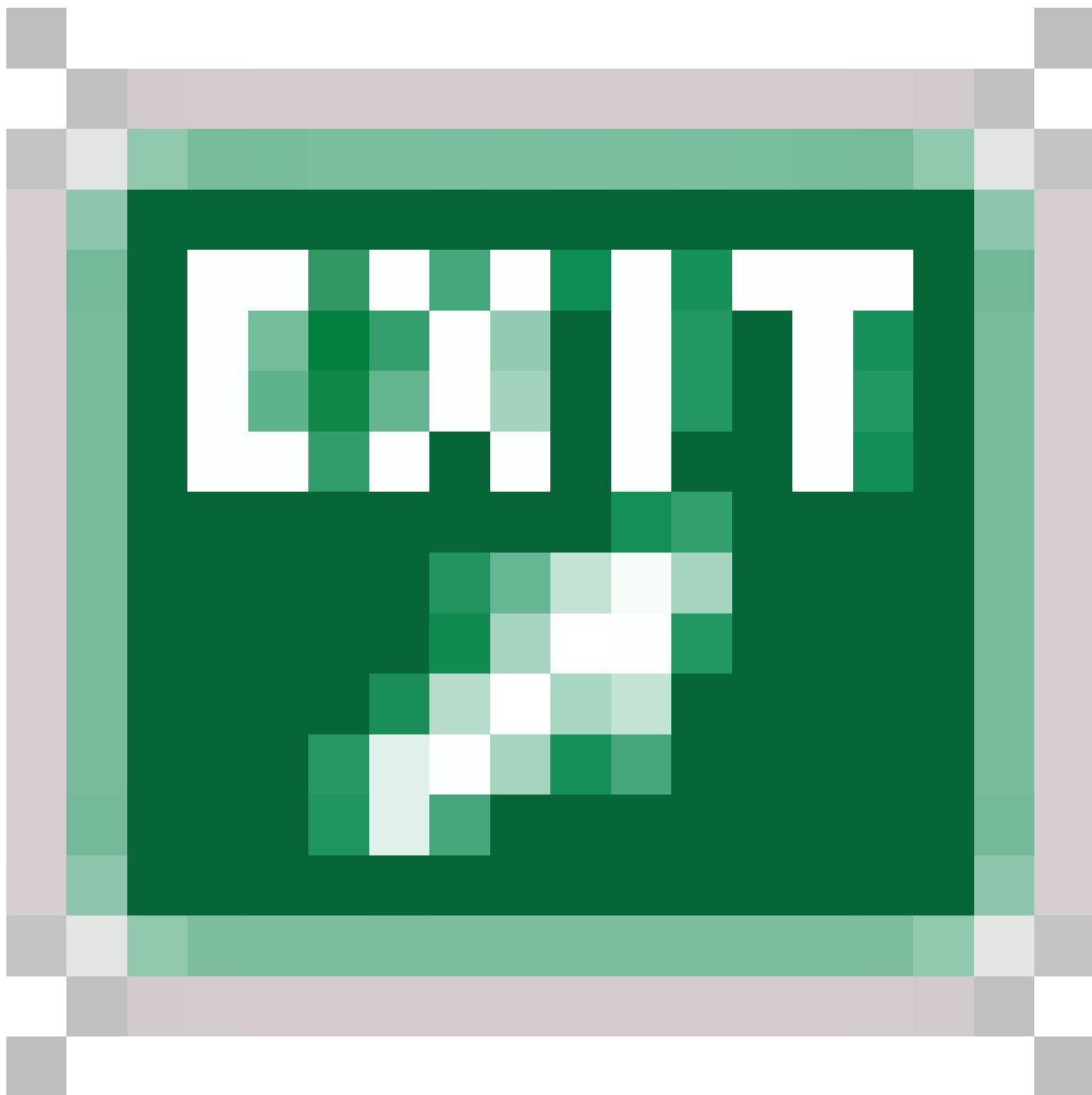
MGCおよび関連製品は、3つの異なるSolarisバージョンで実行されています。

- Solaris 2.5.1
パッチはSunからリリースされていません。
- Solaris 2.6
Solaris 2.6上で稼働するソフトウェアの場合、パッチはCSCOh007.pkgパッケージ内で入手できます。このパッケージは<http://www.cisco.com/pcgi-bin/tablebuild.pl/mgc-sol>からダウンロードできますが、登録ユーザであり、ログインしている必要があります。
- Solaris 2.8
Solaris 8で稼働するソフトウェアの場合、このパッチはMGCSOL8-h015パッケージ内で提供されています。このパッケージは<http://www.cisco.com/pcgi-bin/tablebuild.pl/mgc-sol8>からダウンロードできますが、登録ユーザであり、ログインしている必要があります。

Cisco IPマネージャ

BTS10200

お客様は、<http://sunsolve.Sun.COM/pub-cgi/show.pl?target=patches/patch-access>から入手できる最新の推奨Solarisパッチクラスタをインストールする必要があります。



Cisco IOS

次の表の各行は、リリーストレインと、対象のプラットフォームまたは製品について説明しています。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」）とそれぞれの提供予定日が「リビルド」、「暫定」、および「メンテナンス」の各列に示されます。特定の列のリリース（最初の修正リリースより前）よりも前のリリースを実行しているトレインのデバイスは脆弱であることが確認されており、少なくとも示されているリリース（最初の修正リリースより後）または以降のバージョン（最初の修正リリースのラベルより後）にアップグレードする必要があります。

リリースを選択する際は、次の定義を念頭に置いてください。

- メンテナンス

表の特定の行に記載されているラベルについて、十分なテストを実施し、推奨されるリリースを示します。

- リビルド

同じリリース群の以前のメンテナンスリリースまたはメジャーリリースから構成され、特定の不具合に対する修正が含まれています。テストの回数は少なくなりますが、修理に影響を与えるために必要な最小限の変更のみが含まれています。

- Interim

メンテナンスリリース間で定期的に構築され、テストの頻度が少ない暫定リリースは、この脆弱性に対処する適切なリリースが他にない場合にのみ選択し、暫定イメージは、次のメンテナンスリリースが利用可能な状態になった後、できるだけ早くアップグレードする必要があります。暫定リリースは製造工程では入手できず、通常はCisco TACとの事前調整がない限り、CCOからお客様がダウンロードすることはできません。

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。情報が不明な場合は、「[修正済みソフトウェアの取得](#)」セクションの説明に従ってCisco TACにお問い合わせください。

IOSのリリース名および省略形の詳細については、<http://www.cisco.com/warp/public/620/1.html>を参照してください。

リリース群	イメージまたはプラットフォームの説明	修正リリースのアベイラビリティ		
11.0ベースのリリース以前		リビルド	暫定	メンテナンス
10.3	複数のリリースとプラットフォーム	エンジニアリング終了		
		アップグレードを推奨		
11.0	複数のリリースとプラットフォーム	エンジニアリング終了		
		12.0(23)へのアップグレードを推奨		
11.1	すべてのプラットフォームのメジャーリリー	エンジニアリング終了		

	ス	12.0(23)へのアップグレードを推奨
11.1AA		エンジニアリング終了
		12.1(16)へのアップグレードを推奨
11.1CA		エンジニアリング終了
		アップグレードを推奨
11.1CC		エンジニアリング終了
		アップグレードを推奨
11.1CT		エンジニアリング終了
		12.0STへのアップグレードを推奨
11.1IA		エンジニアリング終了
		12.2(10)へのアップグレードを推奨
11.2	すべてのプラットフォームのメジャーリリース	エンジニアリング終了
		12.0(23)へのアップグレードを推奨
11.2BC		エンジニアリング終了
		12.1(16)へのアップグレードを推奨

11.2F		エンジニアリング終了		
		12.0(23)へのアップグレードを推奨		
11.2GS		エンジニアリング終了		
		12.0(23)へのアップグレードを推奨		
11.2P		エンジニアリング終了		
		12.0(23)へのアップグレードを推奨		
11.2SA		エンジニアリング終了		
		12.0Wへのアップグレードを推奨		
11.2WA4		エンジニアリング終了		
		12.0Wへのアップグレードを推奨		
11.2XA		エンジニアリング終了		
		12.0(23)へのアップグレードを推奨		
11.3 ベースのリリース		リビルド	暫定	メンテナンス
11.3	すべてのプラットフォームのメジャーリリース	エンジニアリング終了		
		12.0(23)へのアップグレードを推奨		

11.3AA	ダイヤルプラットフォームおよびアクセスサーバ用ED:5800、5200、5300、7200	未スケジュール
		12.1(16)へのアップグレードを推奨
11.3DA	ISP DSLAM 6200プラットフォームの初期導入トレイン	エンジニアリング終了
		12.3へのアップグレードを推奨
11.3 DB	6400用のISP/Telco/PTT xDSLブロードバンドコンセンレータプラットフォーム(NRP)の初期導入トレイン	エンジニアリング終了
		12.2Bへのアップグレードを推奨
11.3HA	ISR 3300用の短期EDリリース (SONET/SDHルータ)	エンジニアリング終了
		12.0(23)へのアップグレードを推奨
11.3 MA	MC3810機能のみ	エンジニアリング終了
		12.1(16)へのアップグレードを推奨
11.3NA	Voice over IP、メディアコンバージェンス、さまざまなプラットフォーム	エンジニアリング終了(16)
		12.1へのアップグレードを推奨
11.3T	早期導入者向けの豊富な機能を備えた早期導入メジャーリリース	エンジニアリング終了
		12.0(23)へのアップグレードを推奨
11.3XA	uBR7246および2600の	エンジニアリング終了

	導入	12.0(23)へのアップグレードを推奨		
11.3WA4	LightStream 1010	エンジニアリング終了		
		12.0WAへのアップグレードを推奨		
12.0 ベースのリリース		リビルド	暫定	メンテナンス
12.0	すべてのプラットフォーム向けのGeneral Deploymentリリース		12.0 (22.4)	12.0(23)
12.0DA	xDSLサポート：6100、6200	未スケジュール		
		12.2Tへのアップグレードを推奨		
12.0DB	Early Deployment(ED)リリース：Node Switch Processor(NSP)のCisco 6400 Universal Access Concentrator(UAC)をサポートします。	未スケジュール		
		12.2Bへのアップグレードを推奨		
12.0DC	Early Deployment(ED)リリース：Node Switch Processor(NSP)のCisco 6400 Universal Access Concentrator(UAC)をサポートします。	未スケジュール		
		12.2Bへのアップグレードを推奨		
12.0S	コア/ISPサポート：GSR、RSP、c7200	12.0(16)S9、12.0(21)S3	12.0(21.4)S、12.0(22.3)S1	12.0(22)S

12.0SC	ケーブル/ブロードバンドISP:uBR7200	未スケジュール		
		12.1(13)EC1へのアップグレードを推奨		
12.0SL	10000 ESR:c10k	未スケジュール		
		12.0(23)S3へのアップグレードを推奨		
12.0SP	Early Deploymentリリース	12.0(21)SP1		
12.0ST	Cisco IOSソフトウェアリリース12.0STは、サービスプロバイダー(ISP)向けのCisco 7200、7500/7000RSP、および12000(GSR)シリーズルータ用のEarly Deployment (ED ; 初期配備) リリースです。	12.0(21)ST3		
12.0SY	Early Deploymentリリース	12.0(21.4)SY		12.0(22)SY
12.0T	Early Deployment(ED):VPN、Distributed Director、各種プラットフォーム	未スケジュール		
		12.1(16)へのアップグレードを推奨		
12.0W	Catalystスイッチ : cat8510c、cat8540c、c6msm、ls1010、cat8510m、cat8540m			12.0(24)W5(26)

12.0W	Catalystスイッチ : cat2948g、cat4232			12.0(25)W5(27)
12.0W	Catalystスイッチ : cat5000ATM			12.0(24)W5(26a)
12.0WC		12.0(5)WC5a		
12.0WT	cat4840g (推奨)	未スケジュール		
		アップグレードの決定		
12.0XA	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール		
		12.1(16)へのアップグレードを推奨		
12.0XB	短期初期配備リリース	未スケジュール		
		12.1(16)へのアップグレードを推奨		
12.0XC	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール		
		12.1(16)へのアップグレードを推奨		
12.0XD	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール		
		12.1(16)へのアップグレードを推奨		
12.0XE	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール		
		12.1(8b)E14へのアップグレードを推奨		

12.0XF	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール
		12.1(16)へのアップグレードを推奨
12.0XG	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール
		12.1(16)へのアップグレードを推奨
12.0XH	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール
		12.1(16)へのアップグレードを推奨
12.0XI	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール
		12.1(16)へのアップグレードを推奨
12.0XJ	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール
		12.1(16)へのアップグレードを推奨
12.0(5)XK	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール
		12.1(16)へのアップグレードを推奨
12.0(7)XK	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール
		12.2(10)へのアップグレードを推奨
12.0XL	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール

		12.1(16)へのアップグレードを推奨
12.0XM	Early Deployment(ED) : 限られたプラットフォーム	未スケジュール
		12.2(8)Tへのアップグレードを推奨
12.0XN	Early Deployment(ED) : 限られたプラットフォーム	未スケジュール
		12.1(16)へのアップグレードを推奨
12.0XP	Early Deployment(ED) : 限られたプラットフォーム	未スケジュール
		12.0(5)WC5aへのアップグレードを推奨
12.0XQ	Early Deployment(ED) : 限られたプラットフォーム	未スケジュール
		12.1(16)へのアップグレードを推奨
12.0XR	Early Deployment(ED) : 限られたプラットフォーム	未スケジュール
		12.2(10)へのアップグレードを推奨
12.0XS	Early Deployment(ED) : 限られたプラットフォーム	エンジニアリング終了
		12.1(8b)E14へのアップグレードを推奨
12.0XU	Early Deployment(ED) : 限られたプラットフォーム	未スケジュール
		12.0(05)WC05aへのアップグレードを推奨

12.0XV	Early Deployment(ED) : 限られたプラットフォーム	未スケジュール		
		12.2(10)へのアップグレードを推奨		
12.1 ベースのリリース		リビルド	暫定	メンテナンス
12.1	すべてのプラットフォーム向けの一般導入リリース		12.1(15.3)	12.1(16)
12.1AA	ダイヤルサポート	未スケジュール		
		12.2(10)へのアップグレードを推奨		
12.1DA	xDSLサポート : 6100、6200	未スケジュール		
		12.2Tへのアップグレードを推奨		
12.1DB	Cisco IOSソフトウェアリリース12.1(1)DBは、Cisco 6400ユニバーサルアクセスコンセントレータをサポートします			12.2(15)B
12.1DC	Cisco IOSソフトウェアリリース12.1(1)DCは、Cisco 6400ユニバーサルアクセスコンセントレータをサポートします			12.2(15)B
12.1E	エンタープライズ	12.1(8b)E14、	12.1(12.5)E、	12.1(19)E

		12.1(12c)E1	12.1(18.1)E	
12.1EA	Catalyst 3550			12.1(11)EA1
12.1EC	12.1ECは、uBR7200プラットフォームの新機能の早期サポートと、将来の新しいユニバーサルブロードバンドルータヘッドエンドプラットフォームのサポートを可能にするために提供されています。		12.1(12.5)EC	12.1(13)EC1
12.1EV	Early Deploymentリリース	12.1(10)EV1b		12.1(10)EV4
12.1EW	Cisco 4000シリーズの早期導入			12.1(12c)EW
12.1(1)EX	Catalyst 6000のサポート			12.1(8b)E14
12.1(10)EX	Cisco 7300シリーズの早期導入			12.1(13)EX
12.1EY	Cat8510c、Cat8510m、Cat8540c、Cat8540m、LS1010	未スケジュール		
		12.1(19)Eへのアップグレードを推奨		
12.1EZ	Early Deployment(ED)：特別なイメージ	12.1(6)EZ8		

12.1T	Early Deployment(ED):VPN、 Distributed Director、各 種プラットフォーム	未スケジュール
		12.2(10)へのアップグレードを推奨
12.1XA	Early Deployment(ED)：限ら れたプラットフォーム	未スケジュール
		12.2(10)へのアップグレードを推奨
12.1XB	Early Deployment(ED)：限ら れたプラットフォーム	未スケジュール
		12.2(10)へのアップグレードを推奨
12.1XC	Early Deployment(ED)：限ら れたプラットフォーム	未スケジュール
		12.2(10)へのアップグレードを推奨
12.1XD	Early Deployment(ED)：限ら れたプラットフォーム	未スケジュール
		12.2(10)へのアップグレードを推奨
12.1XF	Early Deployment(ED):811お よび813 (c800イメー ジ)	未スケジュール
		12.2(10)へのアップグレードを推奨
12.1XG	早期導入(ED):800、 805、820、および1600	未スケジュール
		12.2(8)Tへのアップグレードを推奨
12.1XH	Early Deployment(ED)：限ら	未スケジュール

	れたプラットフォーム	12.2(10)へのアップグレードを推奨
12.1XI	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール
		12.2(10)へのアップグレードを推奨
12.1XJ	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール
		アップグレードを推奨
12.1XK	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール
		アップグレードを推奨
12.1XL	Early Deployment(ED) : 限ら れたプラットフォーム	未スケジュール
		12.2(10)へのアップグレードを推奨
12.1XM	短期初期配備リリース	未スケジュール
		12.2(8)Tへのアップグレードを推奨
12.1XP	Early Deployment(ED):1700お よびSOHO	未スケジュール
		アップグレードを推奨
12.1XQ	短期初期配備リリース	未スケジュール
		12.2(10)へのアップグレードを推奨

12.1XR	短期初期配備リリース	エンジニアリング終了
		12.2(8)Tへの移行を推奨
12.1XS	短期初期配備リリース	未スケジュール
		推奨される更新
12.1XT	Early Deployment(ED):1700シ リーズ	未スケジュール
		アップグレードを推奨
12.1XU	Early Deployment(ED)：限ら れたプラットフォーム	エンジニアリング終了
		アップグレードを推奨
12.1XV	短期初期配備リリース	未スケジュール
		12.2(8)Tへのアップグレードを推奨
12.1XW	短期初期配備リリース	未スケジュール
		12.3へのアップグレードを推奨
12.1XX	短期初期配備リリース	未スケジュール
		アップグレードを推奨
12.1XY	短期初期配備リリース	未スケジュール

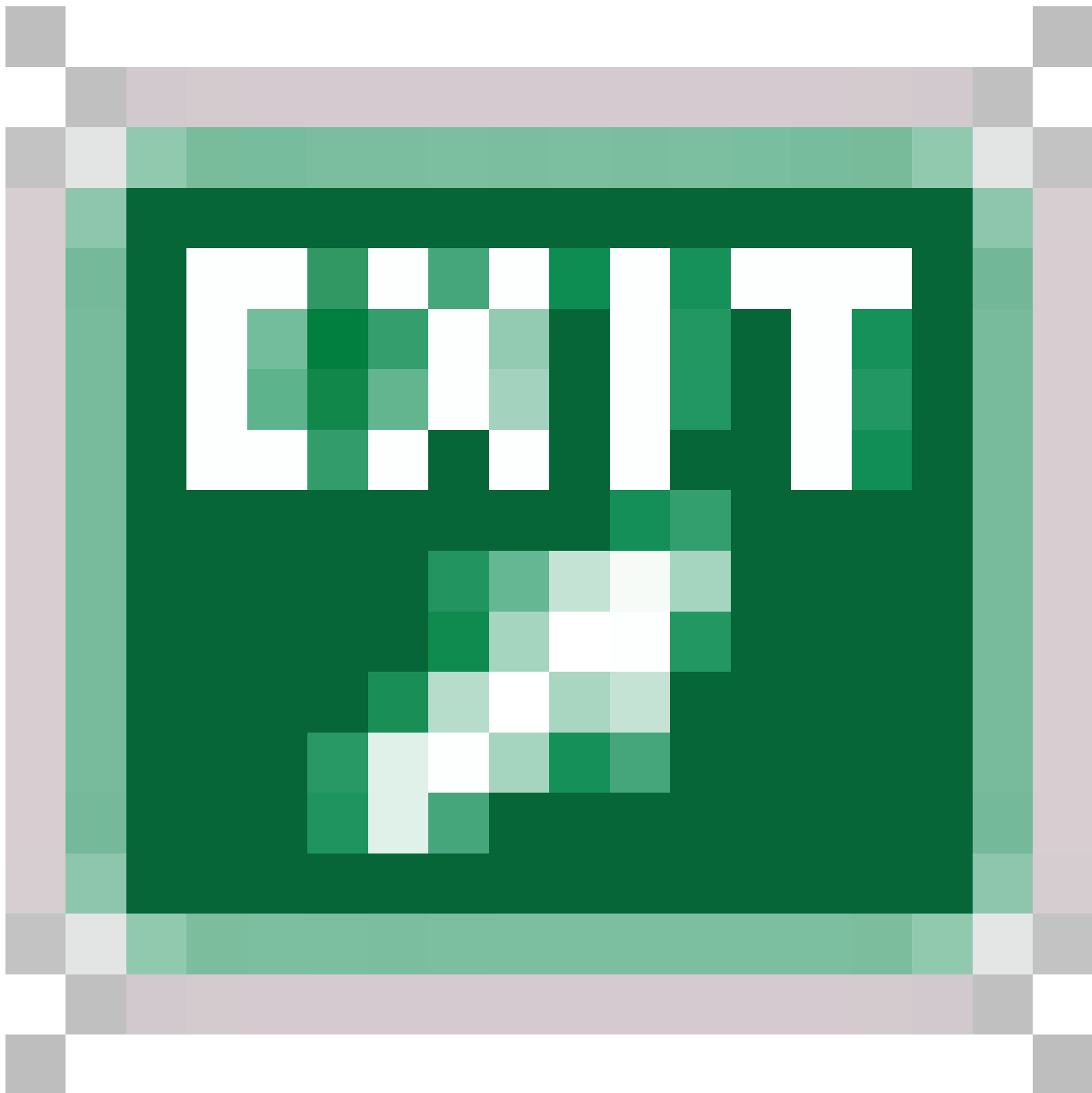
		アップグレードを推奨		
12.1XZ	短期初期配備リリース	未スケジュール		
		アップグレードを推奨		
12.1YA	短期初期配備リリース	未スケジュール		
		アップグレードを推奨		
12.1YB	短期初期配備リリース	未スケジュール		
		アップグレードを推奨		
12.1YC	短期初期配備リリース	未スケジュール		
		12.2(8)Tへのアップグレードを推奨		
12.1YD	短期初期配備リリース	未スケジュール		
		12.2(8)Tへのアップグレードを推奨		
12.1YF	短期初期配備リリース	未スケジュール		
		12.3へのアップグレードを推奨		
12.2 ベースのリリース		リビルド	暫定	メンテナンス
12.2	すべてのプラットフォーム向けの一般導入リリース	12.2(6g)	12.2 (7.4)	12.2(10)

12.2B	6400、7200、7400、ubr10k、ubr7200シリーズ用の特別列車		12.2(7.6)B	12.2(15)B
12.2BX	ブロードバンド専用回線			12.2(15)BX
12.2BW	7200、7400、および7511プラットフォーム用Early Deploymentリリース			12.2(15)BW
12.2DA	6100および6200プラットフォームのxDSLサポート	12.2(9.4)DA		12.2(10)DA
12.2S	コアISPサポート		12.2(7.4)S	12.2(14)S
12.2T	テクノロジートレイン		12.2 (7.4) T	12.2(8)T
12.2XA	SPLOB	未スケジュール		
		12.2(8)Tへのアップグレードを推奨		
12.2XB	短期初期配備リリース	12.2(2)XB7		
12.2XD	短期初期配備リリース	未スケジュール		
		12.2(8)Tへのアップグレードを推奨		
12.2XE	短期初期配備リリース	未スケジュール		

		12.2(8)Tへのアップグレードを推奨		
12.2XH	短期初期配備リリース	未スケジュール		
		12.2(8)Tへのアップグレードを推奨		
12.2XQ	短期初期配備リリース	未スケジュール		
		12.2(11)Tへのアップグレードを推奨		
12.2XZ	短期初期配備リリース	12.2(4)XZ5		
12.2YA	短期リリース	12.2(4)YA3		
12.2YC	短期リリース	12.2(2)YC4		
12.2ZN	短期リリース			12.2(15)ZN
12.3および12.3Tイメージは影響を受けません				
注意事項				
日付はすべて予定であり、変更される可能性があります。 通常のメンテナンス リリースと比較した場合、暫定リリースに対しては厳格なテストが実施されていないため、重大なバグが含まれている可能性があります。				

不正利用事例と公式発表

この脆弱性はPrzemyslaw Frasunekによって発見され、2001年4月4日にBugtraqリストに掲載されました。メールの全文は、<http://www.securityfocus.com/archive/1/174011>で確認できます。この脆弱性は、<http://www.kb.cert.org/vuls/id/970472>



で入手できるCERT/CC vulnerability note VU#970472にも記載されています。

最初の応答は2001年4月12日にBugtraqに送信され、
<http://www.securityfocus.com/archive/1/176137>で確認できます。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020508-ntp-vulnerability>

改訂履歴

Revision 2.1	2003年 10月2日	「ソフトウェアバージョンと修正」 セクションのIOSリリース情報を更 新して追加。
Revision 2.0	2003年 9月22日	新しいバグが追加されました。修正 済みIOSリリースが更新されます。 Solaris 8用のパッチが追加されまし た。
Revision 1.5	2002年 5月16日	「回避策」セクションのアクセスリ ストの構文は修正されました。
リビジョ ン 1.4	2002年 5月15日	「認証にNTPを使用する」回避策を 削除。
リビジョ ン 1.3	2002年 5月13日	「詳細」セクションを更新し、「不 正利用と公表」のCERT/CC脆弱性 ノートVU#970472にURLを追加。
リビジョ ン 1.2	2002年 5月10日	影響を受けない製品を更新して、 Cisco Secure PIX Firewallを含めま した。また、Cisco IOSの最初の回 避策を更新しました。これにより、 IOSはNTPクエリを処理できなくな ります。
リビジョ ン 1.1	2002年 5月9日	影響を受けない製品を追加。
リビジョ ン 1.0	2002年 5月8日	初回公開リリース

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、単独の転載や意識を施した場合、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。

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。