CBOS におけるいくつかの脆弱性

アドバイザリーID : cisco-sa-20001204-cbos
初公開日 : 2000-12-04 08:00
バージョン 1.5 : 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

Cisco 600ファミリルータのオペレーティングシステムであるCBOSでは、複数の脆弱性が確認され、修正されています。

- Webアクセスを許可するように設定されているCisco 600ファミリのルータは、特定のURLを送信することでロックできます。Webアクセスはデフォルトで無効になっており、通常はリモート設定を容易にするために有効になっています。この不具合は、Cisco Bug ID CSCdr98772に記載されています。

- TCP SYNパケットのストリームをルータに送信することで、使用可能なすべてのTCPソケットを使い果たすことができます。その結果、ルータにアドレス指定された新しいTCPセッションは確立されません。この脆弱性とSYNサービス拒否攻撃の違いは、この攻撃は低速のパケットストリーム（1秒あたり1つ）で実行できる点です。この不具合は、Cisco Bug ID CSCds59206に記載されています。

- Webインターフェイスを使用した無効なログイン試行は記録されません。この不具合は、Cisco Bug ID CSCds19142に記載されています。

- 大きなICMP ECHO(PING)パケットをルータに送信することで、ルータをロックアップすることができます。この不具合は、Cisco Bug ID CSCds23921に記載されています。

CBOSの次のリリースは、すべての不具合に対して脆弱です：2.0.1、2.1.0、2.1.0a、2.2.0、2.2.1、2.2.1a、2.3、2.3.2、2.3.5、2.3.7、および2.3.8。

これらの不具合は、2.3.5.015、2.3.7.002、2.3.9、および2.4.1のCBOSリリースで修正されます。この不具合の影響を受けないリリースには、次の「ソフトウェアバージョンと修正」の項に詳細が記載されているようにアップグレードすることをお勧めします。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20001204-cbos で公開されています。

該当製品

このセクションでは、影響を受ける製品の詳細について説明します。

脆弱性のある製品

該当するモデルは、627、633、673、675、675E、677、677i、および678です。

これらのモデルは、2.0.1、2.1.0、2.1.0a、2.2.0、2.2.1、2.2.1a、2.3、2.3.2、2.3.5、2.3.7、および2.3.8のいずれかのCBOSリリースを実行している場合に脆弱になります。

これらの不具合は、2.3.5.015、2.3.7.002、2.3.9、および2.4.1のCBOSリリースで修正されます。

脆弱性を含んでいないことが確認された製品

その他のCBOSソフトウェアリリースは、この脆弱性の影響を受けません。他のシスコ製品はこの脆弱性の影響を受けません。

詳細

0.CSCdr98772

この動作は、CBOSでの不適切なURL解析が原因で発生します。各URLは、少なくとも1つのスペース文字（ASCIIコード32、10進数）で終了することが想定されていました。終端がスペースではないURLを送信すると、CBOSは無限ループに入ります。動作を再開するには、ルータの電源を再投入する必要があります。この脆弱性を不正利用するには、Web接続を受け入れるようにルータを設定する必要があります。Webアクセスパスワードを設定しても、この脆弱性に対する保護は提供されません。

0.CSCds59206

ルータにアドレス指定されたSYNパケットのストリームを送信することで、CBOS内で使用可能なすべてのTCPソケットを使い果たすことができます。これは、CBOSのメモリリークが原因です。ルータが新しい接続を受け入れることができない状態に設定されている場合、ルータがリブートされるまでSYNパケットの低速ストリームによってこの状態を維持できます。ストリームは1秒あたり1パケット程度の低速になる可能性があるため、64 KBの接続を持つ1台のマシンで約150台のルータを保持できます。

注：これは非TCPトラフィックには影響しません。すべてのUser Datagram Protocol（UDP；ユーザデータグラムプロトコル）パケットとInternet Control Message Protocol（ICMP；インター

ネット制御メッセージプロトコル）パケットは、ルータによって問題なく処理できます。ルータを経由するすべての既存および新規のTCPセッションは影響を受けません。

攻撃ストリームが終了すると、ルータは数分以内に自動的に回復します。

0.CSCds19142

Cisco Web Managementインターフェイスを使用すると、パスワードの試行が記録されずにアクセスパスワードを推測し続けることができます。パスワードは「exec-only」または「enable」のいずれかです。「exec-only」パスワードを持つユーザは、ルータ設定を変更できません。

CSCds23921：大きい(サイズが65500バイト以上)ICMP ECHO(PING)パケットをルータ自体に送信することによって、内部変数がオーバーフローし、ルータがロックアップする可能性があります。ルータは、ルータを経由してルーティングされるパケットの影響を受けません。

回避策

0.CSCdr98772

この脆弱性には2つの回避策があります。ルータへのWebアクセスを正規のIPアドレスに制限することで、悪用の可能性を低減できます。

これを行うには、enableモードで次のコマンドを入力します。

```
<#root>

cbos#

set web remote 10.0.0.1

cbos#

set web enabled
```

ここで、10.0.0.1は、ルータへのWebアクセスを正当に必要とするホストのアドレスです。

また、Webアクセスを完全に無効にすることで、この脆弱性の不正利用を防ぐこともできます。これは、イネーブルモードで次のコマンドを入力することで実行できます。

```
<#root>

cbos#

set web disabled
```

もう1つのオプションは、Webポートをデフォルトポートの80から任意のポートに変更することです。これは、悪意のあるプログラムがデフォルトポートにHTTP要求を行っている場合にも役立ちます。これは、次のコマンドを使用して実行できます。

```
<#root>

cbos#

set web port



cbos#

write

cbos#

reboot
```

変更を有効にするには、ルータをリブートする必要があります。また、RFC1700で説明されている既知のポートを回避するように注意する必要があります。

0.CSCds59206

この脆弱性に対する回避策はありません。

0.CSCds19142

Web管理インターフェイスを無効にするには、enableモードで次のコマンドを入力します。

```
<#root>

cbos#

set web disabled
```

0.CSCds23921

ルータ自体を宛先とするすべての着信ICMPエコー(PING)パケットを拒否する必要があります。これは、次のコマンドを使用して実行できます。

```
<#root>
```

```
cbos#
set filter number on deny incoming all 0.0.0.0 0.0.0.0
            255.255.255.255 protocol ICMP
cbos#
set filter number+1 on deny incoming all 0.0.0.0 0.0.0.0
            255.255.255.255 protocol ICMP
```

numberは0 ~ 17の間の空きフィルタ番号です。

修正済みソフトウェア

次の表に、この通知に記載された不具合の影響を受けるCBOSソフトウェアリリースと、対応する最初の修正済みリリースが提供される予定日を示します。日程は暫定的なものであり、変更されることがあります。

メジャー リリース	説明またはプラットフォーム	修正済みリリースの入手可能性*	
		パッチリリース**	一般提供(GA)
All releases	627、633、673、675、677、678	2.3.5.015 2000-DEC-15	-
2.3.7.001	677i	2.3.7.002	-

		2000-DEC-15	
All releases	すべてのプラットフォーム	-	2.3.9 2001年3月19日
All releases	すべてのプラットフォーム	-	2.4.1 2000-DEC-15
注意事項			
*すべての日付は概算であり、変更される可能性があります。 **パッチリリースは、通常のGAリリースほど厳密なテストの対象とはならず、重大なバグが存在する可能性があります。			

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

この脆弱性CSCdr98772は複数のお客様によって発見されました。また、パブリックフォーラムでも議論されました。PSIRTは、この脆弱性がin vivoで不正利用されたというレポートを受け取っています。

脆弱性CSCds23921はお客様によって発見されました。他の2つの脆弱性(CSCds59206とCSCds19142)は、シスコの社内テストで発見されたものです。

Cisco Product Security Incident Response Team(PSIRT)では、CSCds59206、CSCds19142、CSCds23921の公式発表は確認しておりません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20001204-cbos

改訂履歴

1.5	2001年8月8日	「回避策」の項のアップデート.
1.4	2001年3月19日	リリース2.3.9のGAを更新し、ステータスをinterimからfinalに変更しました。
1.3	2000年12月19日	固定ソフトウェアイメージに一時的にアクセスする手順を削除。Cisco 600ルータのWebアクセスに関するCSCdr98772の下のテキストを削除。
1.2	2000-December-13	ソフトウェアの入手可能日を更新し、ソフトウェアの入手手順を追加。
1.1	2000-December-10	ソフトウェアの入手可能日を更新し、「修正済みソフトウェアの入手」セクションにサードパーティサポート組織からの支援を要求する手順を追加。
1.0	2000年12月3日	初版リリースのドラフト。

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。

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。