Cisco 7xx TCPおよびHTTPの脆弱性

アドバイザリーID : cisco-sa-19990311-xxconn
初公開日 : 1999-03-11 16:00
バージョン 1.1 : 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

この通知は、Cisco 7xxシリーズのスモールオフィスおよびホームオフィス(SOHO)ルータで使用されるソフトウェアにおける、2つの無関係なセキュリティの脆弱性に対処するものです。これらの脆弱性は、7xxシリーズのルータにのみ影響し（7xxxシリーズには影響しません）、その他のシスコ製品には影響しません。

1つ目の脆弱性はCisco Bug ID CSCdm03231が割り当てられているため、ルータのTELNETポートへのTCP接続を使用して、システムのリロードを引き起こし、サービス拒否を引き起こすことができます。

2つ目の脆弱性にはバグIDは割り当てられていません。ソフトウェアバージョン3.2(5) ~ 4.2(3)を実行する7xxルータは、単純なHTTPサーバをサポートしています。このHTTPサーバはデフォルトで有効になっています。サーバを明示的に無効にしない限り、サーバを使用してルータの設定を変更したり、その設定に関する情報を取得したりできます。これは意図的な動作ですが、お客様が気付かないうちに検出されたように見えるため、この通知で言及されています。

これらの脆弱性の両方に対して、設定上の回避策があります。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19990311-xxconn で公開されています。

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

これらの脆弱性の影響を受けるのは、7xxシリーズのsmall-office/home-office（SOHO；スモー

ルオフィス/ホームオフィス）ルータが組み込まれたネットワークだけです。7xxルータは、ISDN BRI回線を使用する小規模なリモートネットワークにネットワーク接続を提供するように設計されています。ネットワークに7xxシリーズのルータが含まれている場合、それらのルータはネットワークユーザの自宅や、従業員が少ないリモートオフィスで見つかる可能性が高くなります。

CSCdm03231の影響を受けるのは、リリース4.2(3)以前の任意のソフトウェアバージョンを実行しているすべてのCisco 7xxルータです。これらのルータの管理者は、着信TCP接続をフィルタリングする特定の手順を実行していません。このようなフィルタリングは、デフォルトでは有効になっていません。

HTTPサーバは、3.2(5)から4.2(3)までのすべてのソフトウェアリリースに含まれています。これらすべてのソフトウェアバージョンでは、サーバはデフォルトで有効になっています。

脆弱性を含んでいないことが確認された製品

リリース4.3(1)以降のソフトウェアを実行しているルータは、CSCdm03231の影響を受けません。

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

詳細

CSCdm03231は、4.3(1)より前のすべてのソフトウェアバージョンに影響します。76xまたは77xルータをご使用のお客様は、リリース4.3(1)にアップグレードする必要があります。メモリの制限により、リリース4.3は75xルータではサポートされていません。75xルータをご使用のお客様は、「回避策」セクションで説明されているようにIPフィルタリングを使用する必要があります。

HTTPサーバは、3.2(5)から4.2(3)までのすべてのソフトウェアバージョンに存在します。3.2(4)以前のリリースにも、4.3にも存在しません。76xまたは77xルータをご使用のお客様は、リリース4.3(1)にアップグレードする必要があります。これは主に、CSCdm03231修正プログラムのインストールが望ましいためです。HTTPサーバは、どのソフトウェアバージョンでも無効にすることができます。75xルータを使用するお客様には、サーバを無効にすることをお勧めします。

回避策

このセクションでは、これらの脆弱性の回避策について説明します

CSCdm03231 のための回避策

信頼CSCdm03231きないホストからルータへの着信TCP接続を防止することで、攻撃者にとって非常に役に立たなくなる可能性があります。これは、次の例のようにset ip filter profileコマンドを使用して実行できます。

```
set ip filter tcp source = not trusted-host destination = router block
```

この例では、単一の信頼できる管理ホストからの着信TCP接続だけを受け入れるようにルータを設定します。より複雑な設定、さまざまなホストからのさまざまなタイプの接続の許可が可能です。詳細については、ルータのドキュメントを参照してください。

HTTPサーバの無効化

HTTPサーバを無効にするには、システムコマンドset clickstart offを使用します。

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。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

シスコは、この通知の日付より前にCSCdm03231の発表や議論が行われていないことを認識しています。シスコには、CSCdm03231の悪意のあるエクスプロイトに関する報告はありません。CSCdm03231は、ラボテスト中に外部のセキュリティ会社によって発見されました。

CSCdm03231を効果的に利用するには、簡単なプログラムが必要です。シスコでは、この目的に特化したプログラムが一般に公開されていないことはわかっていますが、そのようなプログラムを作成するために必要な作業はほとんどなく、最も基本的なスキルしか必要としません。また、他の目的で公開されている特定のプログラムが、この脆弱性を悪用するために使用されたり、改変されたりする可能性があります。

シスコには、7xxシリーズのHTTPサーバの不正使用に関する報告はありません。ただし、悪用の可能性については製品ドキュメントで説明されており、潜在的な攻撃者に知られているものと見なす必要があります。

URL

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

19990311-xxconn

改訂履歴

リビジョン 1.1	1999-3-11	初回公開リリース

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。