CBOS Web ベース設定ユーティリティの脆弱性

アドバイザリーID : cisco-sa-20010823-cbos-webserver
初公開日 : 2001-08-23 04:00
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

Cisco 600ファミリルータ用のオペレーティングシステムであるCisco Broadband Operating System(CBOS)では、複数の脆弱性が確認され、修正されています。Cisco 600シリーズファミリのルータは、ルータのWebベースの設定ユーティリティにアクセスする大量のHTTPトラフィックによって応答しなくなる可能性があります。さらに、Webベースの設定ユーティリティはデフォルトで有効になっています。この問題は、Cisco Bug ID CSCdv06084、CSCdv06088、CSCdv06089、およびCSCdv06098に記述されています。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010823-cbos-webserver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

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

これらのモデルでは、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、2.3.8、2.3.9、2.4.1、2.4.2、および2.4.2apのいずれかが稼働している場合に脆弱性が存在します。

これらの不具合は、2.4.2bおよび2.4.3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.CSCdv06084

Cisco 600シリーズルータに複数の接続を介してTelnetでアクセスすると、ルータはトラフィックの受け渡しに失敗し、設定の試行に応答しなくなり、通常の動作に戻るためにリブートが必要になる場合があります。

0.CSCdv06088

Cisco 600シリーズルータが複数の接続を介してHTTP経由でアクセスされると、ルータはトラフィックを渡すことができず、設定の試行に応答しなくなり、通常の動作に戻るためにリブートする必要が生じることがあります。

0.CSCdv06089

Cisco Broadband Operating System(CBOS)のWebベースの設定ユーティリティは、Webベースの設定サービスが無効になっている場合でも、それ自体をTCPポート（別のポートが設定されていない限り、ポート80）にバインドします。このため、影響を受けるサービスが明らかに無効になっている場合でも、Cisco 600シリーズルータはCSCdv06088に対して脆弱になります。

0.CSCdv06098

Webベースのユーティリティはデフォルトで無効になっているため、お客様はこの設定オプションを有効にすることができます。

回避策

これらの脆弱性のそれぞれに対する特別な回避策はありませんが、CodeRedワーム攻撃に対して妥当な防御策であることが証明された回避策が存在します。Web管理ポートを1024より大きい数値に設定し、ポート80のWeb管理を無効にすることを推奨します。次のコマンドを使用して、「number_greater-than_1024」というテキストを実際の数値に置き換えます。

<#root>

set web port *number_greater-than_1024*

修正済みソフトウェア

次の表に、このアドバイザリに記載された脆弱性の影響を受ける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。

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
		一般提供(GA)
All releases	すべてのプラットフォーム	2.4.3 2001年8月23日

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

この問題の不正利用は頻繁に行われており、多くの発表やメッセージが公表されています。最も一般的な不正利用の発生は、CodeRedワームの拡散によるものです。次のような参考資料があります。

- http://www.cert.org/advisories/CA-2001-19.html
- http://www.eeye.com/html/Research/Advisories/AD20010618.html

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010823-cbos-webserver

改訂履歴

リビジョン 1.1	2001年12月6日	「修正済みソフトウェアの取得」セクションを更新
リビジョン 1.0	2001年8月23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。