VTY認証バイパスの脆弱性

アドバイザリーID : cisco-sa-20070829-vty
初公開日 : 2007-08-29 18:00
バージョン 1.2 : 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

これは、NileSOFTセキュリティアドバイザリ『Cisco Catalyst 3750でのバイパス認証の脆弱性12.2(25)』に対するCisco PSIRTの回答です。2007年8月29日、1800 UTC(GMT)に掲載されました。

元の勧告は韓国のウェブサイトに掲載された。

この脆弱性は、2005年4月にお客様によって発見および報告されており、Cisco Bug IDの内容は2005年4月以降、Cisco.comで公開されています。これはプラットフォームに依存しない脆弱性であり、Catalyst 3750デバイスだけに限定されるものではありません。

この脆弱性は、Cisco Bug ID CSCsa91175(登録ユーザ専用)に記載されています。

このCisco Security Responseは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20070829-vtyで公開されています。

追加情報

Cisco Bug ID CSCsa91175(登録ユーザ専用)のリリースノートエンクロージャの内容を次に示します。

症状

認証、認可、アカウンティング(AAA)がデバイスで有効にされておらず、VTY/AUXまたはコンソール回線の下に設定を入力すると(loginコマンドを除く)、VTY回線の下にコマンド「no login」が表示されます。

条件

この症状が発生するのは、デバイスでAAAが有効になっておらず、設定が上記の「症状の説明」

に従って変更された場合だけです。コマンド「no login」が設定に表示されますが、実行コンフィギュレーションがNVRAMに保存され、デバイスがリロードされるまで、デバイスには脆弱性が存在しません。

Cisco Bug ID CSCsa91175(登録ユーザ専用)が統合されていない場合、12.2 E、F、およびSリリース群のCisco IOS®ソフトウェアリリースが影響を受けます。シスコでは、デバイスの設定をチェックして、VTY回線に「no login」コマンドが設定されていないことを確認することを推奨しています。これが望ましい設定である場合は除きます。該当するトレインと最初の修正済みリリースのリストを次に示します。

影響を受けるリリース:	最初の修正リリース：
12.2E based trains EW EWA EU EX EY	Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Fixed in 12.2(35)EX Fixed in 12.2(37)EY
12.2F based trains FX FY FZ	Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround
12.2S based trains S SB SBC SE SEA SEB SEC SED SEE SEF SEG SG SV SW SXD SXE SZ	Vulnerable; apply workaround Fixed in 12.2(31)SB Vulnerable; apply workaround Fixed in 12.2(35)SE Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Fixed in 12.2(31)SG Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Fixed in 12.2(18)SXE4 and later Vulnerable; apply workaround

他のCisco IOSリリーストレインにおいてこの脆弱性の影響を受けるものは確認されていません。

「リリース」および「トレイン」という用語の詳細については、次のURLを参照してください。

http://www.cisco.com/web/about/security/intelligence/ios-ref.html

デバイスの設定を確認するには、デバイスにログインし、特権コマンド「show running-config」を入力します。必要な設定でない限り、VTY回線でコマンド「no login」が設定されていないことを確認します。

「login」コマンドについての詳細は、次を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/tersv_r/ter_l1g.htm#wp998262

パスワードプロンプトなしでリモートターミナルアクセスを許可するデバイスの例を次に示します。

<#root>

```
Device#
show running-config

  <lines removed>
  line VTY 0 4
    no login
  <lines removed>
```

回避策

「login」を使用してVTY回線を設定すると、リモートアクセスではまずパスワードの入力が求められます。

シスコでは、ベストプラクティスとして、可能な限り実用的なSSHへの移行を推奨しています。

注：AAAが設定されている場合、loginコマンドで使用される追加コマンドについては、AAA設定ガイドを参照してください。

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の説明も含まれています。すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070829-vty

改訂履歴

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。