Cisco IOSリモートルータのクラッシュ

アドバイザリーID : cisco-sa-19980810-ios-login
初公開日 : 1998-08-10 16:00
バージョン 1.4 : 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 IOSソフトウェアにエラーがあると、信頼されていない未認証のユーザが、ルータや他のCisco IOSデバイスのログインプロンプトに何らかの方法でアクセスし、デバイスのクラッシュやリロードを引き起こす可能性があります。

これは、従来のCisco IOSソフトウェアを実行しているデバイスにのみ適用されます。これには、シスコのルータ製品のほとんどが含まれますが、すべてではありません。デバイスが従来のCisco IOSソフトウェアを実行しているかどうかを確認する最も簡単な方法は、次の「影響を受けるユーザ」で説明するshow versionコマンドを使用することです。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19980810-ios-login 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

従来のCisco IOSソフトウェアバージョン9.1以降を使用していて、このNoticeの「詳細」セクションに記載されている修復バージョンよりも前のユーザは、この脆弱性の影響を受けます。これらのユーザのデバイスは、信頼できないユーザによってインタラクティブに接続されている可能性があります。この脆弱性を悪用するために実際にログインする必要はありません。端末接続を確立するだけで十分です。この脆弱性は、ログインプロンプトを含む、ルータによって発行される任意のインタラクティブプロンプトから不正利用される可能性があります。

修正済みソフトウェアの一部はフィールドにしばらく存在します。すでにインストールされて

いる可能性があります。該当すると判断する前に、ソフトウェアのバージョン番号を確認してください。

この脆弱性は、直接コンソールまたは非同期シリアル接続（ダイヤルアップ接続を含む）、TELNET接続、UNIX「r」コマンド接続、LAT接続、MOP接続、X.29接続、V.120接続などを使用して不正利用される可能性があります。例外的なセキュリティ環境を除き、悪意のあるユーザがCisco IOSデバイスにインタラクティブな接続を行う方法を見つけることができると想定することを強くお勧めします。

すべてのシスコ製品をこのNoticeに記載することは不可能です。使用しているデバイスが従来のCisco IOSソフトウェアを実行しているかどうかわからない場合は、デバイスにログインしてshow versionコマンドを発行します。従来のCisco IOSソフトウェアは単に「IOS」または「Internetwork Operating System Software」と表示され、該当するソフトウェアのバージョン番号は9.1以上になります。他のシスコデバイスには、show versionコマンドがないか、異なる出力が返されます。

脆弱性を含んでいないことが確認された製品

従来のCisco IOSソフトウェアを実行していない場合は、この脆弱性の影響を受けません。従来のCisco IOSソフトウェアを実行しないCiscoデバイスには、次のものがあります。

- 7xxダイヤルアップルータ（750、760、および770シリーズ）は該当しません。
- Catalyst LANスイッチ（Catalyst 2900XLを除く）は、この脆弱性の影響を受けません。
- IGXまたはBPXラインのWANスイッチング製品は影響を受けません。
- AXISシェルフは該当しません。
- LS1010またはLS2020 ATMスイッチは該当しません。このNoticeの以前のバージョンでは、一部のLS1010スイッチが影響を受けていると報告されていました。これは工ラーでした。LS1010スイッチで使用されているCisco IOSソフトウェアの11.2WAxおよび11.3WAxバージョンは、修復されたバリアントに基づいています。
- ホストベースのソフトウェアには脆弱性はありません。
- Cisco PIX Firewallには脆弱性はありません。
- Cisco LocalDirectorには脆弱性は存在しません。
- Cisco Cache Engineには脆弱性はありません。

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

Cisco IOSソフトウェアエラーには、Cisco Bug ID CSCdj43337が割り当てられています。

注：CCOの登録ユーザで、ログインしている場合は、バグの詳細を表示できます。

回避策

Cisco IOSデバイスへのインタラクティブアクセスを防止することで、この問題を回避できます。IPベースのインタラクティブアクセスだけが問題になる場合は、ip access-class回線設定を使用して、システム内のすべての仮想端末にアクセスリストを適用します。ただし、Cisco IOSデバイスへのインタラクティブな接続を行う非IPベースの手段は存在することを覚えておき、攻撃の可能なルートとしてこれらの手段を排除することが重要です。インタラクティブアクセスを完全に防止するには、設定コマンドno execを任意の非同期回線に適用するか、コマンドtransport input noneを任意の仮想端末回線に適用します。仮想端末回線は、信頼できないユーザがアクセスできる可能性があります。

修正済みソフトウェア

この脆弱性は、9.1から次の修正済みリリース（暫定およびベータ版ソフトウェアを含む）までのクラシックCisco IOSソフトウェアのすべてのリリースに影響します。

- 11.3(1)、11.3(1)ED、11.3(1)T
- 11.2(10)、11.2(9)P、11.2(9)XA、11.2(10)BC、11.2(8)SA3
- 11.1(15)CA、11.1(16)、11.1(16)IA、11.1(16)AA、11.1(17)CC、11.1(17)CT
- 11.0（20.3）

上記の特定のリリースを実行する必要はありません。この修正は、同じリリースの後続のすべてのバージョンにも存在します。たとえば、11.2(9)Pは固定されているため、11.2(10)Pも固定されています。

Cisco IOSソフトウェアの10.3以前のリリースはサポートが終了しており、現在のところ、それらのリリースに対して修正が提供される予定はありません。ただし、9.1以降のすべてのリリースには問題があります。

Cisco IOSソフトウェアに対して計画されているすべての修正が完了し、テストされています。11.0を除くすべてのバージョンで、正規リリースのソフトウェアへの統合が完了しています。上記よりも古いバージョンのソフトウェアを実行している場合は、Cisco TACに連絡して支援を求めてください。

この通知の日付の時点で、この問題の修正は11.0(20.3)バージョンの11.0リリースでのみ利用可能です。これは暫定リリースであり、通常のCisco IOSリリースと同等のテストは行われていません。修正を含む最初の通常の11.0リリースは11.0(21)です。11.0(21)のリリースは1998年9月中旬を予定しています。このスケジュールは変更される可能性があります。11.0 Cisco IOSソフトウェアは比較的完成度が高いため、11.0(20.3)をインストールした方が、新しいCisco IOSバージョンの暫定リリースをインストールするよりもリスクが低いと考えられます。重要なデバイスに11.0(20.3)またはその他の暫定リリースをインストールする場合は注意が必要です。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

シスコには、この脆弱性の悪意のあるエクスプロイトに関する実際の報告はありません。ただし、この脆弱性によって引き起こされたクラッシュと一致する、説明のつかないクラッシュが散発的に報告されています。この脆弱性は、このようなレポートによって最初に特定されたものです。報告されたクラッシュがランダムなイベントによって引き起こされた可能性もありますが、意図的であった可能性もあります。どちらのケースが当てはまるかを判断するのに役立つ情報は、シスコには基本的に何もありません。クラッシュを報告したお客様の中に、意図的な攻撃の疑いを示すものはありませんでした。

シスコでは、この通知の日付より前には、この脆弱性に関する公式発表はありません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19980810-ios-login

改訂履歴

リビジョン 1.4	1998年 8月20日	LS1010スイッチへの影響に関するエラーを修正。11.2(8)SA3が修復バージョンリストに追加されました。
リビジョン 1.3	1998年 8月19日	さまざまな一般的な誤解が修正されました。脆弱性が存在するCisco IOSソフトウェアバージョンと、従来のCisco IOSソフトウェアを実行する製品に関する詳細情報。
リビジョン 1.2	1998年 8月10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。