

Cisco IOS HTTPサーバのpingパラメータにおけるクロスサイトスクリプティングの脆弱性



アドバイザリーID : Cisco-SA-20090114- [CVE-2008-3821](#)
CVE-2008-3821 [3821](#)
初公開日 : 2009-01-14 16:58
バージョン 1.0 : Final
CVSSスコア : [4.3](#)
回避策 : No Workarounds available
Cisco バグ ID : [CSCsi13344](#) [CSCsr72301](#)

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ソフトウェアには脆弱性があり、認証されていないリモートの攻撃者がユーザのブラウザセッションで任意のHTMLおよびスクリプトコードを実行する可能性があります。

この脆弱性は、組み込みHTTPサーバでの入力サニタイズエラーが原因で発生します。認証されていないリモートの攻撃者は、この脆弱性を不正利用して、悪意のあるリンクを追跡するようにユーザを誘導する可能性があります。このアクションにより、攻撃者はユーザのブラウザセッションで任意のHTMLおよびスクリプトコードを実行できる可能性があります。

シスコはこの脆弱性を確認し、更新されたソフトウェアをリリースしました。

この脆弱性は、Cisco IOSソフトウェアの組み込みHTTPサーバのエラーが原因で発生します。セキュリティ上のベストプラクティスにより、管理者はこのサーバを使用していないときは無効にするよう定められています。ネットワークを確認して、組み込みHTTPサーバを実行しているCisco IOSデバイスの目的を確認することをお勧めします。

該当製品

シスコは、Cisco Bug ID [CSCsi13344](#)に対処するセキュリティ応答を次のリンクでリリースしました。 [cisco-sr-20090114-http](#)

脆弱性のある製品

組み込みHTTPサーバが有効になっている状態で稼働するCisco IOSシステムには、脆弱性が存在する可能性があります。お客様は、サポート組織に連絡して、ソフトウェアバージョンに脆弱性があるかどうかを確認することをお勧めします。

脆弱性を含んでいないことが確認された製品

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。

回避策

適切なアップデートを適用することを推奨します。

HTTPサーバが業務に必要な場合は、無効にすることを推奨します。詳細については、『Cisco Guide to Harden Cisco IOS Devices』ドキュメントの「[Disable Unused Services](#)」セクションを参照してください。

管理者は、アクセスコントロールリスト(ACL)を適用して、HTTPサーバへのアクセスを制限することを推奨します。

未承諾のリンクは使用しないことをお勧めします。ユーザは、予期しないリンクを追跡する前に、その信頼性を確認する必要があります。

Cisco Applied Intelligenceチームは、管理者がこの脆弱性を悪用しようとする攻撃を識別して緩和できるように、関連する次のドキュメントを作成しました。このドキュメントは、更新されたソフトウェアを適用する前に確認できます。[cisco-amb-20060922-understanding-xss](#)

修正済みソフトウェア

契約が有効なシスコのお客様は、[Cisco](#)のSoftware Centerからアップデートを入手できます。契約をご利用でないお客様は、1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)にお問い合わせいただくか、tac@cisco.comのEメールでアップグレードを入手できます。

推奨事項

```
$propertyAndFields.get("recommendations")
```

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA->

改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|-------|--------|-------|-------|------------|
| 1.0 | 初版リリース | 適用外 | Final | 2009年1月14日 |

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。