

Xauth Internet Key Exchange (IKE) 実装の脆弱性

severity アドバイザリーID : cisco-sa- [CVE-20050406-xauth](#)
初公開日 : 2005-04-06 16:00 [2005-1057](#)
バージョン 1.1 : Final [CVE-2005-1058](#)
回避策 : [Yes](#)
Cisco バグ ID : [CSCeg00277](#) , [CSCin82407](#)

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インターネットワーク オペレーティング システム (IOS) ソフトウェア リリーストレイン 12.2T、12.3 および 12.3T はインターネット キー エクスチェンジ (IKE) Xauth ある特定のメッセージの処理で脆弱性が含まれているかもしれません Easy VPN Server であるために設定されたとき。

これらの脆弱性の不正利用の成功は割り当て許可されていないユーザ 認証を完了し、可能性としてはネットワークリソースにアクセスするかもしれません。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050406-xauth> に掲示されます

シスコでは、該当するお客様用に、この脆弱性に対応する無償ソフトウェアを提供しております。

該当製品

修正済みソフトウェア

この問題はサポートする影響を与え、のために、Cisco Easy VPN サーバ Xauth バージョン 6 認証設定されます Cisco IOS の取りはずされたバージョンを実行するすべての Cisco デバイスに。

Easy VPN Server を実行し、Xauth 認証のために設定された Cisco デバイスは設定の次の行を

備えています:

```
crypto map <mapname> client authentication list <listname>
```

Easy VPN Server Xauth機能はまたに類似した 設定によって ISAKMP プロファイルの下に有効になるかもしれません:

```
crypto isakmp profile <profilename>
  match identity group <groupname>
  client authentication list <listname>
  isakmp authentication list <listname>
  client configuration address respond
  qos-group 2
```

デバイスに Cisco製品、ログインで動作するソフトウェアを判別し、システムバナーを表示するために「show version」コマンドを発行するため。Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。出力次の行で、イメージ名は「バージョンに」先行しているかこと IOSリリース名の間で表示する。その他の Cisco 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。

次の例は C3640-I-M のインストール済みイメージ名前と IOS リリース 12.3(6) を実行する Cisco製品を指定したものです:

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-I-M), Version 12.3(6), RELEASE SOFTWARE (fc3)
```

次の例は C3845-ADVIPSERVICESK9-M のイメージ名と IOS リリース 12.3(11)T3 を実行する製品を示します:

```
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.3(11)T3, RELEASE
SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

Cisco IOS リリース指名についてのその他の情報は

<http://www.cisco.com/warp/public/620/1.html> で見つけることができます。

脆弱性を含んでいないことが確認された製品

Cisco Easy VPN サーバは IOS だけ機能です。IOS を実行しないデバイスは脆弱ではありません。

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。

改訂履歴

リビジョン 1.0	2005-April-6	初回公開リリース
--------------	--------------	----------

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。