Cisco IOS OSPFの悪用

Informational

アドバイザリーID : cisco-sa-20030220-ospf
初公開日 : 2002-02-23 08:00
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

これは Cisco セキュリティ アドバイザリではありません。

この文書は、シスコのお客様用のパブリック フォーラムに掲載された、製品セキュリティの潜在的な脆弱性の問題に対するシスコの回答へのアクセスを容易にするために提供されています。これは、シスコがこれらの各問題を実際の製品セキュリティの脆弱性として認識していることを意味するものではありません。この通知は「現状のまま」で提供されるものであり、いかなる約束または保証を意味するものでもありません。このページの情報またはこのページからリンクされている資料は、お客様ご自身の責任においてご利用ください。シスコは、いつでも予告なしに、このページを変更またはアップデートする権利を留保します。

追加情報

元のレポートは、http://www.securityfocus.com/archive/1/312510にあります（Cisco IOSソフトウェアリリース12.1T以降ではサポートされていません）。 シスコは、次の内容を回答しました。この回答も http://www.securityfocus.com/archive/1/312802 にアーカイブされています。

シスコは、2003年2月20日に投稿されたPhenoelitのメッセージ「Cisco IOS OSPF exploit」でFXが行ったステートメントを確認できます。特定のCisco IOS®ソフトウェアバージョンでのOpen Shortest Path First(OSPF)の実装は、255を超えるホストがインターフェイスごとにネイバー関係の確立を試行するネイバー通知のフラッドを受信した場合、サービス拒否の脆弱性があります。

この問題の回避策の1つは、OSPF MD5認証を設定することです。これは、インターフェイスごとまたはエリアごとに実行できます。詳細については、http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtmlでMD5認証の設定に関するドキュメントを参照してください。

もう1つの回避策として、次に示すように、着信アクセスリストを適用して、特定のOSPFネイバーだけを明示的に許可する方法があります。

```
access-list 100 permit ospf host a.b.c.x host 224.0.0.5
access-list 100 permit ospf host a.b.c.x host interface_ip
access-list 100 permit ospf host a.b.c.y host 224.0.0.5
access-list 100 permit ospf host a.b.c.y host interface_ip
access-list 100 permit ospf host a.b.c.z host 224.0.0.5
access-list 100 permit ospf host a.b.c.z host interface_ip
access-list 100 permit ospf any host 224.0.0.6
access-list 100 deny ospf any any
access-list 100 permit ip any any
```

Cisco IOSソフトウェアバージョン11.1 ~ 12.0は、この脆弱性の影響を受けます。このバグは解決されています。Cisco IOSソフトウェアの次のバージョンは最初の修正済みリリースです。つまり、後続のリリースにも修正が含まれています。

- 12.0(19)S
- 12.0(19)ST
- 12.1(1)
- 12.1(1)DB
- 12.1(1)DC
- 12.1(1)T

FXは、今後とも責任ある情報開示の精神に基づき、セキュリティ問題の認識を高めていくことを目指し、ご協力を賜りますよう、お願い申し上げます。

潜在的なセキュリティ問題に関するCisco PSIRTとの連携については、https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.htmlの連絡先情報を参照してください。

この問題は、当初Bugtraqメーリングリストのhttp://www.securityfocus.com/archive/1/312510で報告され、シスコはhttp://www.securityfocus.com/archive/1/312802で対応し、この通知が送信されました。

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-20030220-ospf

改訂履歴

バージョン	説明	セクション	日付
リビジョン 1.1	最終更新日：		2004年7月19日
リビジョン 1.0	初回公開リリース		2003年2月20日

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。