Cisco Nexus 5000および3000シリーズスイッチのアクセスコントロールリストバイパスの脆弱性

アドバイザリーID : cisco-sa-20110907-nexus
初公開日 : 2011-09-07 16:00
バージョン 1.0 : 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 Nexus 5000および3000シリーズスイッチには、デバイスに設定されているアクセスコントロールリスト(ACL)のdeny文をトラフィックがバイパスする可能性のある脆弱性が存在します。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。

この脆弱性を軽減する回避策があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110907-nexus で公開されています。

該当製品

Cisco Nexus 5000および3000シリーズスイッチは、ACLのdenyステートメントの前にremarkが設定されている場合、この脆弱性の影響を受けます。

脆弱性のある製品

Cisco Nexus 5000 NX-OSソフトウェアリリース5.0(2)および5.0(3)の5.0(3)N2(1)より前のバージョンはすべて、この脆弱性の影響を受けます。

注：Cisco Nexus 5000 NX-OSソフトウェアリリース4.xはこの脆弱性の影響を受けません。

Cisco Nexus 3000 NX-OSソフトウェアリリース5.0(3)U1(2a)または5.0(3)U2(1)より前のリリースはすべて、この脆弱性の影響を受けます。

この脆弱性の影響は、ACLのdenyステートメントの前にACLの注釈が設定されている場合に発生します。注釈は、設定されているアクセスコントロールエントリ(ACE)に関するコメントです。

次の例は、IPv4 ACLで注釈を作成し、結果を表示する方法を示しています。

```
ip access-list acl-ipv4-01
 remark this ACL denies the 10.1.1.0/24 access to the 10.1.2.0/24 network
 deny ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
```

注：注釈の後のすべてのACEが影響を受けます。これには、ACLの最後のデフォルトの暗黙のdenyが含まれます。IPv4、IPv6、およびMAC ACLが影響を受けます。Quality of Service(QoS)分類およびルートマップACLは、この脆弱性の影響を受けません。

ソフトウェアバージョンの確認

シスコ製品で実行されているCisco NX-OSソフトウェアリリースは、管理者がデバイスにログインして、show versionコマンドを発行することにより確認できます。次の例は、Cisco NX-OSリリース5.0(2)N2(1)を実行しているデバイスで実行されているキックスタートイメージとシステムイメージのバージョン情報を表示する方法を示しています。

```
<#root>

switch#

show version


Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2010, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.3.0
  loader:    version N/A
  kickstart: version 5.0(2)N2(1) [build 5.0(2)N2(1)]
  system:    version 5.0(2)N2(1) [build 5.0(2)N2(1)]


!--- output truncated
```

脆弱性を含んでいないことが確認された製品

次のシスコ製品はこの脆弱性の影響を受けないことが確認されています。

- Cisco Nexus 7000 Series Switches
- Cisco Nexus 4000 シリーズ スイッチ
- Cisco Nexus 2000 シリーズ スイッチ ページ
- Cisco Nexus 1000V シリーズ スイッチ
- Cisco MDS 9000ソフトウェア
- Cisco Unified Computing System

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

ACLは、トラフィックをフィルタリングする順序付きルールのセットです。各ルールは、パケットがルールに一致するために満たす必要がある一連の条件を指定します。デバイスは、ACLがパケットに適用されると判断すると、すべてのルールの条件に対してパケットをテストします。最初に一致したルールによって、パケットが許可されるか拒否されるかが決まります。一致するルールがない場合、デバイスは該当する暗黙的ルールを適用します。デバイスは、許可されたパケットの処理を続行し、拒否されたパケットをドロップします。

Cisco Nexus 5000および3000シリーズスイッチの脆弱性により、デバイスに設定されているIP、VLAN、またはMAC ACLのdenyステートメントをトラフィックがバイパスする可能性があります。この動作は、そのようなACLのdenyステートメントの前にACLの注釈が設定されている場合に発生します。

注：注釈の後のすべてのACEが影響を受けます。これには、ACLの最後のデフォルトの暗黙のdenyが含まれます。IPv4、IPv6、およびMAC ACLが影響を受けます。QoS分類およびルートマップACLは、この脆弱性の影響を受けません。

この脆弱性は、Cisco Bug ID CSCto09813（登録ユーザ専用）およびCSCtr61490(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2011-2581が割り当てられています。

回避策

この脆弱性の影響は、ACLの denyステートメントの前にACLの注釈が設定されている場合に発生します。回避策として、この脆弱性を緩和するために設定からコメントを削除できます。ACLの注釈を削除するには、設定されている各ACLの下で no remarkコマンドを使用します。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco Nexus 3000 NX-OSソフトウェア

この脆弱性は、Cisco Nexus 3000 NX-OSソフトウェアリリース5.0(3)U1(2a)または5.0(3)U2(1)以降ですでに修正されています。

Cisco Nexus 3000 NX-OSソフトウェアは、次のリンク先からダウンロードできます。
http://www.cisco.com/cisco/software/find.html?q=nx-os

Cisco Nexus 5000 NX-OSソフトウェア

この脆弱性は、Cisco Nexus 5000 NX-OSソフトウェアリリース5.0(3)N2(1)以降で修正されています。

Cisco Nexus 5000 NX-OSソフトウェアは、次のリンク先からダウンロードできます。
http://www.cisco.com/cisco/software/find.html?q=nx-os

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

この脆弱性は、カスタマーサービスリクエストのトラブルシューティング中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110907-nexus

改訂履歴

リビジョン 1.0	2011年9月7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。