Cisco Security Advisory: Cisco Nexus 5000 and 3000 Series Switches Access Control List Bypass Vulnerability

Advisory ID: cisco-sa-20110907-nexus

http://www.cisco.com/warp/public/707/cisco-sa-20110907-nexus.shtml

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。

Revision 1.0

For Public Release 2011 September 07 1600 UTC (GMT)

目次

要約

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たアクセス コントロール リスト（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無償のソフトウェア アップデートをリリースしました。

この脆弱性には回避策があります。

このアドバイザリは次のリンクに掲載されます。 http://www.cisco.com/warp/public/707/cisco-sa-20110907-nexus.shtml

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コメントが設定されている場合に、この脆弱性の影響を受けます。

脆弱性が存在する製品

Cisco Nexus 5000 NX-OS ソフトウェア リリース 5.0(2) および 5.0(3) のすべて（つまり、5.0(3)N2(1) よりも前のバージョン）が、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。

また、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) よりも前のバージョンがすべて、この脆弱性の影響を受けます。

ACL のどの **deny** ステートメントの前であっても、ACL コメントを設定するとこの脆弱性の影響を受けます。コメントは、設定したアクセス コントロール エントリ（ACE）に関するコメントのことです。

次の例は、IPv4 ACL でコメントを作成し、結果を表示した場合を示しています。

```
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：コメントに続く ACE はすべて影響を受けます。これには、ACL の末尾にあるデフォルトの暗黙の deny も含まれます。IPv4、IPv6、および MAC ACL が影響を受けます。Quality of Service（QoS）分類と route-map 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

シスコ製品で稼動している Cisco NX-OS ソフトウェア リリースを確認するには、デバイスにログインし、 **show version** コマンドを実行してシステム バナーを表示させます。次の例は、Cisco NX-OS リリース 5.0(2)N2(1) が稼動するデバイス上で実行されているキックスタート イメージおよびシステム イメージ ファイルのバージョン情報の表示を示しています。

```
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
```

脆弱性が存在しない製品

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 シリーズ スイッチ
- Cisco Nexus 4000 シリーズ スイッチ
- Cisco Nexus 2000 シリーズ スイッチ
- 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するためのルールを定めたセットです。各ルールには、パケットがルールと一致するために満たすべき条件のセットが指定されています。デバイスが、あるパケットに ACL が適用されると判断すると、デバイスはすべてのルールの条件に関してパケットを検証します。最初に適用されるルールにより、パケットの許可または拒否が判断されます。これに一致しない場合、デバイスは適用可能な暗黙のルールを適用します。このようにして、デバイスは許可されたパケットを処理し、拒否されたパケットを廃棄していきます。

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た 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ことがあります。このような動作は、ACL の任意の **deny** ステートメント前に ACL コメントが設定されている場合に起こります。

注：コメントに続く ACE はすべて影響を受けます。これには、ACL の末尾にあるデフォルトの暗黙の deny も含まれます。IPv4、IPv6、および MAC ACL が影響を受けます。QoS 分類と route-map 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（ 登録ユーザのみ ）および CSCtr61490（ 登録ユーザのみ ）として文書化され、CVE ID CVE-2011-2581 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、個々のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次の URL にて CVSS に関する FAQ を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを以下の URL にて提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x

CSCto09813 and CSCtr61490 - Access Control List Bypass Vulnerability Calculate the environmental score of					
CVSS Base Score - **5**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	None	None
CVSS Temporal Score - **4.1**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用に成功した場合、攻撃者は Cisco Nexus 5000 および 3000 シリーズ スイッチに設定された ACL によって保護されるべきリソースにアクセスできる可能性があります。

ソフトウェア バージョンおよび修正

ソフトウェアのアップグレードを検討する際には、 http://www.cisco.com/go/psirt/ および本アドバイザリ以降に公開のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

いずれの場合も、アップグレードするデバイス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。情報が不明確な場合は、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

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、次の場所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) 以降ですでに修正されています。

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

回避策

ACL のどの **deny** ステートメントの前であっても ACL コメントを設定すると、この脆弱性の影響を受けます。設定からコメントを削除することで、この脆弱性を回避できます。ACL コメントは、設定された各 ACL で **no remark** コマンドを使用して削除できます。

修正済みソフトウェアの入手

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。ソフトウェアの導入を行う前にお客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項、または Cisco.com ダウンロード サイトの http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他の条項に従うことに同意したことになります。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、シスコのワールドワイド Web サイト上の Software Center からアップグレードを入手することができます。 http://www.cisco.com

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、本脆弱性に関する適切な処置について指示と支援を受けてください。

回避策の効果は、使用製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品が多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。TAC の連絡先は次のとおりです。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このお知らせの URL をご用意ください。サービス契約をご利用でないお客様に対する無償アップグレードは、TAC 経由でご要求いただく必要があります。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、 http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html を参照してください。

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とその公表は確認しておりません。

この脆弱性は、お客様のサービス リクエストへの対応中に発見されました。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

本アドバイザリは、次のシスコのワールドワイド Web サイト上に掲載されます。

http://www.cisco.com/warp/public/707/cisco-sa-20110907-nexus.shtml

ワールドワイド Web 以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものもシスコのワールドワイド Web サイトに掲載される予定です。しかしながら、前述のメーリング リストもしくはニュースグループに対し積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最新情報をご確認いただくことをお勧めいたします。

更新履歴

Revision 1.0	2011-September-07	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、シスコ ワールドワイド Web サイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。このページには、シスコのセキュリティ通知に関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは http://www.cisco.com/go/psirt/ で確認することができます。