Cisco Security Advisory: Cisco NX-OS Malformed IP Packet Denial of Service Vulnerability

Advisory ID: cisco-sa-20120215-nxos

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120215-nxos/

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 2.0

Last Updated 2012 March 26 21:02 UTC (GMT)

For Public Release 2012 February 15 16:00 UTC (GMT)

目次

要約

Cisco NX-OS ソフトウェアはサービス拒否（DoS）の脆弱性の影響を受けます。該当するバージョンの Cisco NX-OS ソフトウェアが稼働している Cisco Nexus 1000V、1010、5000、7000 シリーズ スイッチ、および Nexus 1000V シリーズ スイッチ用の Cisco Virtual Security Gateway (VSG) で IP スタックが不正な IP パケットを処理した場合、デバイスが再起動する可能性があります。

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。

このアドバイザリは、次のリンク先で確認できます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120215-nxos/

該当製品

脆弱性が存在する製品

該当するバージョンの Cisco NX-OS ソフトウェアが稼働している Cisco Nexus 1000V、1010、5000、7000 シリーズ スイッチおよび Nexus 1000V シリーズ スイッチ用の Cisco VSG は、この脆弱性の影響を受けます。この脆弱性はオペレーティング システムの IP スタック内に存在するため、 IP スタックで提供されるサービスを利用して IP パケットを処理する機能は いずれも影響を受けます。

最初の修正リリースより前の Cisco NX-OS ソフトウェア バージョンは脆弱性の影響を受けます。修正バージョンについては、「ソフトウェア バージョンおよび修正」セクションを参照してください。

Cisco Nexus スイッチで稼働している Cisco NX-OS ソフトウェアのバージョンを確認するには、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 5.1(3) が稼働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
Documents:
http://www.cisco.com/en/US/products/ps9372/tsd_products_support_
serie
s_home.html
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights
reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
  BIOS:      version 3.22.0
  kickstart: version 5.1(3)
  system:    version 5.1(3)

[...]
```

脆弱性が存在しない製品

Cisco Nexus 1000V、1010、5000、7000 シリーズ スイッチおよび Nexus 1000V シリーズ スイッチ用の Cisco VSG 以外の Cisco NX-OS ソフトウェアは、この脆弱性の影響を受けません。特に、Cisco NX-OS ソフトウェアが稼働していても次の製品は影響を受けません。

- Cisco Nexus 2000 シリーズ スイッチ
- Cisco Nexus 3000 シリーズ スイッチ
- Cisco Nexus 4000 シリーズ スイッチ
- Unified Computing System (UCS)

- Cisco MDS 9000 シリーズ マルチレイヤ スイッチ

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

Cisco NX-OS ソフトウェアはシスコ製品で使用されるネットワーク オペレーティング システムであり、Cisco Nexus 5000 シリーズや Cisco Nexus 7000 シリーズなどのデータセンター スイッチを含むシスコ データセンター スイッチング ポートフォリオに含まれます。

Cisco Nexus 1000V、1010、5000、7000 シリーズ スイッチおよび Nexus 1000V シリーズ スイッチ用の Cisco Virtual Security Gateway (VSG) で稼働する Cisco NX-OS ソフトウェアの特定のバージョンが脆弱性の影響を受けます。該当するデバイスは、オペレーティング システムの IP スタックで不正な IP パケットが処理され、 パケットからレイヤ 4 (UDP または TCP) 情報が取得されると、再起動する可能性があります。

この脆弱性はオペレーティング システムの IP スタック内に存在するため、 IP スタックで提供されるサービスを利用して IP パケットを解析する機能は いずれも影響を受けます。たとえば、次のシナリオでは、 設定された機能を実行するためにレイヤ 4 (UDP または TCP) の 情報を必要とするため、脆弱性が引き起こされる可能性があります。

- スイッチによって通常は転送される不正な通過 IP パケットを受信し、その存続可能時間 (TTL) が 1 の場合。このようなケースでは、ICMP エラー メッセージ (時間超過) を生成する必要があり、 この ICMP メッセージの生成中にバグが引き起こされる可能性があります。
- ポリシーベース ルーティングを使用しており、ルーティングを決定するときに着信パケットを解析する必要がある場合。パケットが不正な TCP セグメントであり、ルーティングを決定する際にルーティング ポリシーが TCP 情報を使用する場合、このバグが引き起こされる可能性があります。
- 出力アクセス コントロール リスト (ACL) がインターフェイスに適用されており、そのインターフェイスから転送された不正な IP パケットを受信した場合。

注： これはすべてを網羅した完全なリストではありません。リストには、このドキュメントに説明のある脆弱性を引き起こすことが確認されているいくつかのシナリオが含まれています。このほか、不正な IP パケットのレイヤ 4 情報にアクセスが必要なシナリオでも、脆弱性が引き起こされる可能性があります。

この脆弱性は、デバイスを通過するトラフィックとデバイス宛のトラフィックのどちらでも引き起こされる可能性があります。IP アドレスが設定されている該当 Cisco Nexus スイッチは、IP アドレスが管理目的でのみ使用されていたり、デバイスが純粋なレイヤ 2 スイッチ (つまりレイヤ 3 パケットの転送を行わない) として構成されている場合でも、この脆弱性の影響を受けます。

この脆弱性によって再起動されたシステムは、「netstack」というプロセスによって予期せず停止し、システム ログには次のメッセージが記録されます。

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents:
http://www.cisco.com/en/US/products/ps9372/tsd_products_support_
serie
s_home.html
```

```
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights
reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
  BIOS:      version 3.22.0
  kickstart: version 5.1(3)
  system:    version 5.1(3)

[...]
```

この脆弱性は、Cisco Bug ID CSCti23447 （登録ユーザのみ）、CSCti49507 （登録ユーザのみ）（Cisco Nexus 1000V および 7000 シリーズ）、CSCtj01991 （登録ユーザのみ）（Cisco Nexus 5000 シリーズ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2012-0352 が割り当てられています。

注：Cisco Nexus 1000V および 7000 シリーズ スイッチの脆弱性については、Cisco Bug CSCti23447 で一部が修正されていることから、2 つの Cisco Bug ID でトラッキングされています。修正は CSCti49507 で完了しました。Cisco Nexus 5000 シリーズ スイッチについては、Cisco Bug CSCtj01991 で完全に脆弱性が修正されました。

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組織の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、自身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。シスコは次のリンクで CVSS に関する追加情報を提供しています。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 計算ツールを次のリンクで提供しています。

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

CSCti23447, CSCti49507, CSCtj01991 **Calculate the environmental score of**					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Netw	Low	None	None	None	Comple

ork					te
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

このアドバイザリに記載された脆弱性の不正利用に成功した場合、該当するデバイスでは再起動が発生することがあります。この脆弱性が繰り返し悪用されると、継続的な DoS 状態とな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場合は、http://www.cisco.com/go/psirt/ の Cisco Security Advisories and Responses アーカイブと、後続のアドバイザリを参照して、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 NX-OS ソフトウェア テーブル（下記）の各行は Cisco NX-OS ソフトウェアのリリース トレインを示します。あるリリース トレインが脆弱である場合、修正を含む最初のリリースは、表の「First Fixed Release」列に示されます（入手可能予想日が示される場合もあります）。実行しているリリースが、そのトレインで「First Fixed Release」以前のものである機器は脆弱であることが知られています。

Platform	Major Release	First Fixed Release
Cisco VSG for Nexus 1000V Series Switches	4.x	4.2(1)VSG1(3.1)
Nexus 1000v Series Switches	4.x	4.2(1)SV1(4b) (available late April 2012) 4.2(1)SV1(5.1)
Nexus 1010 Series Switches	4.x	4.2(1)SP1(4)
Nexus 5000 Series Switches	4.x	Vulnerable; migrate to 5.x
	5.0.x	5.0(2)N1(1)
	5.1.x	Not vulnerable
Nexus 7000 Series Switches	4.2.x	4.2.8
	5.0.x	5.0.5
	5.1.x	5.1.1
	5.2.x	Not vulnerable
	6.x	Not vulnerable

Cisco 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

回避策

このドキュメントに記載されている脆弱性に対する回避策はありません。

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性の 1 つ、または複数の脆弱性に対処する無償のソフトウェア アップデートを提供しています。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。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 または http://www.cisco.com/public/sw-center/sw-usingswc.shtml に記載のシスコのソフトウェア ライセンス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、Cisco.com 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、適切な処置について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。影響製品およびリリース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または修正が最適であるか、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。

- +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、このアドバイザリの 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は TAC を通して無償

アップグレードをお求めください。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、シスコ ワールドワイドお問い合わせ先を参照してください。http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team（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、カスタマー サポート ケース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

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120215-nxos/また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- 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

このアドバイザリに関する今後の更新があれば、Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 2.0	2012-March-26	Added Nexus 1010 and VSG as vulnerable products and included fixed software information for them. Added 4.2(1)SV1(4b) as a first fixed release for Nexus 1000v.
Revisio	2012-February	Added 4.x releases for Nexus 1000v Series Switches as vulnerable.

n 1.1	-17	
Revisio n 1.0	2012-February-15	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、Cisco.com 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 Web ページには、シスコのセキュリティ アドバイザリ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。