Cisco NX-OSにおける不正なIPパケットによるDoS脆弱性

アドバイザリーID : cisco-sa-20120215-nxos
初公開日 : 2012-02-15 16:00
最終更新日 : 2012-03-26 21:02
バージョン 2.0 : Final
回避策 : No Workarounds available
Cisco バグ ID : CSCtj01991 CSCti23447 CSCti49507

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 NX-OSソフトウェアは、Cisco Nexus 1000v、1010、5000、7000シリーズスイッチ、およびCisco NX-OSソフトウェアの該当バージョンを実行し、不正なIPパケットをIPスタックが処理する際にリロードするCisco Virtual Security Gateway(VSG)for Nexus 1000Vシリーズスイッチの原因となるサービス拒否(DoS)の脆弱性ののの影響ををを受します。

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。

このアドバイザリは、次のリンクより確認できます。

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120215-nxos

該当製品

脆弱性のある製品

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Cisco VSG for Nexus 1000Vシリーズスイッチは、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スタックに存在するため、IPスタックが提供するサービスを利用してIPパケットを処理する機能が影響を受けます。

最初の修正済みリリースバージョンよりも前のCisco NX-OSソフトウェアバージョンが影響を

受けます。修正済みバージョンの詳細については、「ソフトウェアバージョンと修正」セクションを参照してください。

Cisco Nexusスイッチで実行されているCisco NX-OSソフトウェアのバージョンを確認するには、管理者がデバイスにログインしてshow versionコマンドを発行し、システムバナーを表示します。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
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)

[...]
```

脆弱性を含んでいないことが確認された製品

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Cisco VSG以外の製品の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する次の製品は影響を受けません。

- Cisco Nexus 2000 シリーズ スイッチ ページ
- Cisco Nexus 3000 Series Switches
- Cisco Nexus 4000 シリーズ スイッチ
- Unified Computing System（UCS）
- Cisco MDS 9000 Series Multilayer Switches

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、シスコのデータセンタースイッチングポートフォリオの一部であるシスコ製品によって使用されるネットワークオペレーティングシステムです。これには、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が含まれます。

Cisco Nexus 1000V、1010、5000、7000シリーズスイッチ用のCisco NX-OSソフトウェアの特定のバージョン、およびNexus 1000Vシリーズスイッチ用のCisco Virtual Security Gateway(VSG)は、オペレーティングシステムのIPスタックが不正なIPパケットを処理し、パケットからレイヤ4（UDPまたはTCP）情報をを取得するする際に、該当デバイスののリロードが発生するするするする脆弱性ののの影響をををを受します。

この脆弱性はオペレーティングシステムのIPスタックに存在し、IPスタックが提供するサービスを使用してIPパケットを解析する機能が影響を受けます。たとえば、次のシナリオは、設定された機能を実行するにはレイヤ4（UDPまたはTCP）情報が必要であることを意味するため、脆弱性をトリガーする可能性があります。

- 通常はスイッチによって転送される不正な形式のトランジットIPパケットが受信され、存続可能時間(TTL)は1です。この場合、ICMP工ラーメッセージ（時間超過）を生成する必要があります。このICMPメッセージの生成中に、バグがトリガーされる可能性があります。
- ポリシーベースルーティングが使用されており、ルーティングを決定するには、着信パケットを解析する必要があります。パケットが不正なTCPセグメントであり、ルーティングポリシーがルーティング決定にTCP情報を使用する場合、このバグがトリガー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、そのインターフェイスを介して転送する必要がある不正なIPパケットが受信されます。

注：このリストは、すべてを網羅しているわけではありません。このドキュメントで説明されている脆弱性を引き起こすことが確認されているシナリオの一部が含まれています。不正なIPパケットのレイヤ4情報へのアクセスを必要とするその他のシナリオでも、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、through-the-device(transit)トラフィックとto-the-deviceトラフィックの両方によって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アドレスが管理のためだけに使用されていて、デバイスが純粋なレイヤ2スイッチとして設定されている（つまり、レイヤ3パケット転送が設定されていない）場合でも、この脆弱性の影響を受けます。

この脆弱性が原因でシステムがリロードすると、「netstack」と呼ばれるプロセスが突然終了し、次のメッセージがシステムログに記録されます。

```
2012 Feb 02 20:32:15 NX-7010 %SYSMGR-2-SERVICE_CRASHED: Service "netstack" (PID 4335)
 hasn't caught signal 11 (core will be saved).
```

この脆弱性は、Cisco Bug ID CSCti23447(登録ユーザ専用)およびCSCti49507(登録ユーザ専用)（Cisco Nexus 1000vおよび7000シリーズ）とCSCtj01991(登録ユーザ専用)（Cisco Nexus 5000シリーズ）として文書化され、Common Vulnerabilities and Exposures(CVE)IDcve-2012-0352。

注：Cisco Nexus 1000vおよび7000シリーズスイッチでは、脆弱性がCisco Bug CSCti23447で部分的に修正されているため、この脆弱性を追跡するために2つのCisco Bug IDが使用されています。修正はCSCti49507で完了しています。Cisco Nexus 5000シリーズスイッチについては、この脆弱性はCisco Bug CSCtj01991で完全に修正されています

回避策

このドキュメントで説明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

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 アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性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規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、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ています。特定のリリーストレインに脆弱性が存在する場合、その修正を含む最初のリリース（および該当する場合は、それぞれでの提供予定日）が表の「最初の修正済みリリース」列に一覧表示されます。特定の列のリリースより前（First Fixed Releaseより前）の特定のトレインのリリースを実行しているデバイスは、脆弱であることが確認されています。

Platform	メジャー リリース	First Fixed Release（修正された最初のリリース）
Nexus 1000Vシリーズスイッチ向けCisco VSG	4.(x)	4.2(1)VSG1(3.1)
Nexus 1000vシリーズスイッチ	4.(x)	4.2(1)SV1(4b)（2012年4月下旬に提供開始） 4.2(1)SV1(5.1)

Nexus 1010 シリーズ スイッチ	4.(x)	4.2(1)SP1(4)
Nexus 5000 シリーズ スイッチ	4.(x)	脆弱性あり、5.xに移行
	5.0.x	5.0(2)N1(1)
	5.1.x	脆弱性なし
Nexus 7000 シリーズ スイッチ	4.2.x	4.2.8
	5.0.x	5.0.5
	5.1.x	5.1.1
	5.2.x	脆弱性なし
	6.x	脆弱性なし

Cisco NX-OSソフトウェアは、次のURL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 Product Security Incident Response Team（PSIRT）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を確認していません。

この脆弱性は、カスタマーサポートケースの調査中に発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120215-nxos

改訂履歴

Revision 2.0	2012年3月26日	Nexus 1010とVSGを脆弱性のある製品として追加し、それらの修正済みソフトウェア情報を含めました。Nexus 1000vの最初の修正済みリリースとして4.2(1)SV1(4b)が追加されました。
リビジョ	2012年	脆弱性のあるNexus 1000vシリーズ

ン 1.1	2月 17日	スイッチの4.xリリースを追加。
リビジョン 1.0	2012年 2月 15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。