Cisco NX-OS ソフトウェアの Pong パケットにおける Denial of Service（DoS）の脆弱性

High

アドバイザリーID： cisco-sa-20180117-nx-os

初公開日： 2018-01-17 16:00

バージョン 1.0： Final

CVSSスコア： 7.4

回避策： No workarounds available

Cisco バグ ID： CSCuv98660

CVE-2018-0102

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 ソフトウェアの Pong ツールの脆弱性により、認証されていない隣接する攻撃者が該当デバイスのリロードを引き起こし、その結果サービス妨害（DoS）状態が発生する可能性があります。

この脆弱性の原因は、該当するソフトウェアがメモリ内の同じ領域を 2 回解放しようとすることにあります。 この脆弱性は、pong 応答パケットが FabricPath ポートと非 FabricPath ポートの両方に出力されるようなネットワーク上の場所から、攻撃者が該当デバイスに pong 要求を送信することで、不正利用される可能性があります。 不正利用されると、攻撃者によってデュアル スーパバイザまたはクワッド スーパバイザ仮想ポートチャネル（vPC）のリロードが引き起こされる可能性があります。

注: この脆弱性は、次の条件がすべて満たされている場合のみ、不正利用が可能になります。

1. 該当デバイスで Pong ツールが有効になっている。 NX-OS で Pong ツールがデフォルトで無効になっている。
2. 該当デバイスで FabricPath 機能が有効になっている。 NX-OS で FabricPath 機能がデフォルトで無効になっている。
3. FabricPath ポートが Switched Port Analyzer（SPAN）セッションを通じてアクティブにモニタされている。 デフォルトでは NX-OS で SPAN セッションが設定または有効化されていない。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。 この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-nx-os

該当製品

脆弱性のある製品

この脆弱性は、次の製品で Cisco NX-OS ソフトウェア リリース 7.2(1)D(1)、7.2(2)D1(1)、または 7.2(2)D1(2) を実行し、Pong と FabricPath 両方の機能を有効にして、SPAN セッションを通じて FabricPath ポートをアクティブにモニタしている場合、影響が現れます。

- Cisco Nexus 7000 Series Switches
- Cisco Nexus 7700 シリーズ スイッチ

Cisco NX-OS システム ソフトウェアの脆弱性のあるリリースがデバイスで実行されているかどうかを管理者が確認するには、NX-OS のコマンドライン インターフェイス (CLI) で **show version** コマンドを使用します。

次の例は Cisco NX-OS ソフトウェア リリース 7.2(2)D1(2) を実行する Cisco Nexus 7000 シリーズ スイッチのための **show version コマンド**の出力を示したものです:

```
Nexus# 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_series_home.html
Copyright (c) 2002-2016, 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 2.12.0
kickstart: version 7.2(2)D1(2)
system:    version 7.2(2)D1(2)
.
.
.
```

デバイスが使用可能になる Pong ツールを備えているかどうか判別するために管理者は **show running-config を**使用できます | NX-OS CLI に **「機能 pong」**コマンドを **含めて下さい。**
Pong ツールが有効になっている Cisco Nexus 7000 シリーズ スイッチでの、このコマンドの出力例を下記に示します (コマンドから空の出力が返される場合は、Pong ツールが無効になっています) 。

```
Nexus# show running-config | include "feature pong"
feature pong
```

デバイスがイネーブルになっている FabricPath 機能を備えているかどうか判別するために管理者は **show running-config を**使用できます **|** NX-OS CLI に **「feature-set fabricpath」**コマンドを **含めて下さい**。 FabricPath 機能が有効になっている Cisco Nexus 7000 シリーズ スイッチでの、このコマンドの出力例を下記に示します（コマンドから空の出力が返される場合は、FabricPath 機能が無効になっています）。

```
Nexus# show running-config | include "feature-set fabricpath"
feature-set fabricpath
```

デバイスが設定される SPANセッションを備えているかどうか判別するために管理者は NX-OS CLI で **show running-config monitor コマンドを**使用できます。 SPAN セッションのモニタリング インターフェイス イーサネット 1/10 が設定され有効になっている Cisco Nexus 7000 シリーズ スイッチでの、このコマンドの出力例を下記に示します（コマンドから空の出力が返される場合は、SPAN セッションが設定されていません）。

```
Nexus# show running-config monitor

!Command: show running-config monitor
!Time: Mon Oct 9 12:04:52 2017

version 7.2(2)D1(2)
monitor session 1
source interface Ethernet1/10 both
destination interface Ethernet1/12
no shut
```

脆弱性を含んでいないことが確認された製品

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。

シスコでは、この脆弱性が Cisco NX-OS ソフトウェアの 7.2(0)D1(1) 以前のリリースには影響しないことを確認しています。

シスコでは、この脆弱性が Cisco マルチレイヤ ディレクタ スイッチには影響しないことを確認しています（このプラットフォームでは該当する NX-OS リリースを使用できないため）。

詳細

Pong ツールはネットワーク上の同期クロックを使用して、リアルタイム レイテンシを測定します。 レイテンシとは、2 点間で伝達されるフレームによって観察される、任意の 2 点間におけるネットワークの遅延を意味します。 Pong はポートツーポートの遅延を測定し、ネットワーク監視ユーティリティ Ping と同様ですが、より詳細なネットワーク診断を提供します。

セキュリティ侵害の痕跡

この脆弱性の不正利用により影響を受けたデバイスは *pong* コア ファイルをリロードし、生成します。 このコア ファイルを確認し、デバイスにこの脆弱性の不正利用が発生していないかを判別するには、Cisco Technical Assistance Center（TAC）までご連絡ください。

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコはこのアドバイザリに記載された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。 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、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載された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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、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。

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 TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この脆弱性は、Cisco NX-OS ソフトウェア リリース 7.3(0)D1(1) 以降で修正されています。

ソフトウェアは Cisco.com の Software Center から **製品 > スイッチ > データセンター スイッチ > Nexus 7000 シリーズ スイッチ**へのによってナビゲート ダウンロードすることができます。

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エクスプロイト事例やその公表を確認していません。

出典

この脆弱性は、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-nx-os

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018 年 1 月 17 日

利用規約