Cisco IOSおよびIOS XEソフトウェアのVLANトランキングプロトコルにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-20180926-vtp CVE-2018-0197
初公開日 : 2018-09-26 16:00
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : Yes
Cisco バグ ID : CSCvd37163

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 IOSソフトウェアおよびCisco IOS XEソフトウェアのVLAN Trunking Protocol(VTP)サブシステムの脆弱性により、認証されていない隣接する攻撃者が該当デバイスの内部VTPデータベースを破損し、サービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、影響を受けるソフトウェアがVTPパケットのサブセットを処理する方法の論理エラーに起因します。攻撃者は、該当ソフトウェアのVTPメッセージ処理コードでタイムアウトをトリガーするシーケンスでVTPパケットを送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はVLANの作成、変更、または削除に影響を与え、DoS状態を引き起こす可能性があります。

本脆弱性に対処する回避策がいくつかあります。

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-20180926-vtp

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアの脆弱性が存在するリリースを実行し、VTPクライアントモードまたはVTPサーバモードで動作し、VTPドメイン名が設定されていないシスコデバイスに影響を与えます。

Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアを実行し、VTPをサポートするシスコデバイスのデフォルト設定では、ドメイン名が設定されていないVTPサーバモードで動作し

ます。

脆弱性が存在する Cisco IOS ソフトウェアおよび IOS XE ソフトウェアのリリースについては、このアドバイザリの「修正済みソフトウェア」の項を参照してください。

VTP設定の確認

VTPの動作モードとVTPドメイン名がデバイスに設定されているかどうかを確認するには、管理者がデバイスにログインして、CLIでshow vtp statusコマンドを使用し、コマンドの出力を参照します。

次に、デフォルト設定を使用しているデバイスでのshow vtp statusコマンドの出力例を示します。この設定は、VTPドメイン名が設定されていないVTPサーバモードで動作します。デバイスでCisco IOSソフトウェアまたはCisco IOS XEソフトウェアの脆弱性が存在するリリースも実行されている場合、そのデバイスはこの脆弱性の影響を受けます。

```
<#root>

Switch#

show vtp status


VTP Version capable             : 1 to 3
VTP version running             : 1

VTP Domain Name                 :

VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0cd9.9675.dd80
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 192.168.88.1 on interface Vl1 (lowest numbered VLAN interface found)

Feature VLAN:
--------------

VTP Operating Mode                : Server

Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                                    0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC

Switch#
```

次の例は、VTPサーバモードで動作しており、VTPドメイン名がMYVTPDOMAINであるデバイスでのshow vtp statusコマンドの出力を示しています。デバイスにVTPドメイン名が設定されているため、デバイスはこの脆弱性の影響を受けません。

```
<#root>
```

```
Switch#
```

show vtp status

```
VTP Version capable             : 1 to 3
VTP version running             : 1
```

VTP Domain Name   : MYVTPDOMAIN

```
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0cd9.9675.dd80
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 192.168.88.1 on interface Vl1 (lowest numbered VLAN interface found)

Feature VLAN:
--------------
```

VTP Operating Mode   : Server

```
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0xFE 0x33 0x43 0x04 0x9D 0x91 0x37 0x58
                                    0x66 0xA0 0x68 0x3F 0x74 0x6A 0x22 0x5B
Switch#
```

Cisco IOS ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS 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、CLI で show version コマンドを使用し、表示されるシステム バナーを参照することにより確認できます。デバイスが Cisco IOS ソフトウェアを実行している場合、システム バナーに「Cisco Internetwork Operating System Software」や「Cisco IOS Software」などのテキストが表示されます。バナーにはインストールされたイメージ名もカッコ内に表示され、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリース名が表示されます。一部のシスコデバイスでは、show version コマンドをサポートしていなかったり、別の出力が表示されたりします。

次に、Cisco IOS ソフトウェア リリース 15.5(2)T1 が実行されていて、インストールされているイメージ名が C2951-UNIVERSALK9-M であるデバイスでのコマンド出力例を示します。

<#root>

```
Router>
```

show version

```
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
.
```

.
.

Cisco IOS ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

Cisco IOS XE ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XE 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、CLI で show version コマンドを実行し、表示されるシステム バナーを参照することにより確認できます。デバイスが Cisco IOS XE ソフトウェアを実行している場合、システム バナーに「Cisco IOS Software」、「Cisco IOS XE Software」などのテキストが表示されます。

次に、Cisco IOS XR ソフトウェア リリース 16.2.1 が実行されていて、インストールされているイメージ名が CAT3K_CAA-UNIVERSALK9-M であるデバイスでのコマンドの出力例を示します。

<#root>

```
ios-xe-device#
```

show version

```
Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali 16.2.1, REL
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が Cisco IOS XR ソフトウェアまたは Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

詳細

この脆弱性は、影響を受けるソフトウェアがVTPパケットのサブセットを処理する方法の論理エラーに起因します。攻撃者は、該当ソフトウェアのVTPメッセージ処理コードでタイムアウトをトリガーするシーケンスでVTPパケットを送信することで、この脆弱性を不正利用する可能性があります。

この脆弱性の不正利用が発生するには、デバイスがトランクポートとして動作しているポートを介してVTPパケットを受信する必要があります。アクセスポートとして動作しているポートで受信されたVTPパケットは、デバイスでは処理されません。

Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアを実行し、VTPをサポートするほとんどのシスコデバイスでは、スイッチポートのデフォルトのポート設定はdynamic autoです。dynamic auto設定のポートは、接続されているデバイスによってトランクポートに変換できます。スイッチポートでこの設定を使用している管理者は、このような動作が必要か望ましいかを判断する必要があります。このように設定されておらず、ポートがホストへのネットワークアクセスを提供するためだけに使用されることが予想される場合、管理者はスイッチポートをスタティックアクセスポートに再設定することを検討する場合があります。

セキュリティ侵害の痕跡

この脆弱性が不正利用されると、次の口ギングメッセージが生成される可能性があります。

```
Aug 29 2018 13:02:57.434 EST: %SW_VLAN-4-VTP_INTERNAL_ERROR: VLAN manager received an internal error 4 from vtp fur
-Traceback= 463F74z 1DE5DE4z 2253E40z 2257D14z 2254C88z 22593C8z 2B0A128z 2B0A194z 225AA28z 225827Cz 2255540z 297DD
Aug 29 2018 13:03:27.445 EST: %SW_VLAN-4-VTP_INTERNAL_ERROR: VLAN manager received an internal error 4 from vtp fur
-Traceback= 463F74z 1DE5DE4z 2253E40z 2257D14z 2254C88z 22593C8z 2B0A128z 2B0A194z 225AA28z 225827Cz 2255540z 297DD
Aug 29 2018 13:03:57.444 EST: %SW_VLAN-4-VTP_INTERNAL_ERROR: VLAN manager received an internal error 4 from vtp fur
-Traceback= 463F74z 1DE5DE4z 2253E40z 2257D14z 2254C88z 22593C8z 2B0A128z 2B0A194z 225AA28z 225827Cz 2255540z 297DD
Aug 29 2018 13:04:27.449 EST: %SW_VLAN-4-VTP_INTERNAL_ERROR: VLAN manager received an internal error 4 from vtp fur
-Traceback= 463F74z 1DE5DE4z 2253E40z 2257D14z 2254C88z 22593C8z 2B0A128z 2B0A194z 225AA28z 225827Cz 2255540z 297DD
```

メッセージは約30秒ごとに発生します。-Traceback= テキストの後に表示される値はバージョンによって異なります。

回避策

この脆弱性の不正利用を防ぐために、管理者はCLIでvtp domain設定コマンドを使用してデバイスのVTPドメイン名を設定できます。

修正済みソフトウェア

該当するソフトウェアリリースと修正済みソフトウェアリリースの詳細については、Cisco IOSソフトウェアチェッカーを参照してください。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（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。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、特定のソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。また該当する場合、そのリリースに関するすべてのアドバイザリの脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用して次のタスクを実行できます。

- ドロップダウン リストからリリース（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- show version コマンドの出力をツールで解析する
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

リリースが、公開されたシスコ セキュリティ アドバイザリのいずれかに該当するかどうかを確認するには、Cisco.com の Cisco IOS Software Checker を使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアリリース（たとえば、15.1(4)M2、3.13.8S など）を入力します。

Check

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[Impact Rating] ドロップダウン リストの [中間（Medium）] チェックボックスをオンにします。

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。

出典

シスコは、この脆弱性を報告していただいたnetworkers.plのMarcin T. Sleczek氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-vtp

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2018 年 9 月 26 日

利用規約

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。