複数のシスコオペレーティングシステムにおける単方向リンク検出のDoS脆弱性

Medium

アドバイザリーID : cisco-sa-ios-nxos-xr-udld-dos-W5hGHgtQ
CVE-2021-34714
初公開日 : 2021-09-22 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 : CSCvw26129 CSCvw22670 CSCvw26130 CSCvw26152 CSCvw46194 CSCvw26126 CSCvw26127 CSCvw46239

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 FXOSソフトウェア、Cisco IOSソフトウェア、Cisco IOS XEソフトウェア、Cisco IOS XRソフトウェア、およびCisco NX-OSソフトウェアの単方向リンク検出(UDLD)機能の脆弱性により、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す可能性があります。

この脆弱性は、UDLDパケットの不適切な入力検証に起因します。攻撃者は、巧妙に細工されたUDLDパケットを該当デバイスに送信することにより、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、攻撃者が該当デバイスをリロードできるようになり、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。

注：UDLD機能はデフォルトで無効になっており、この脆弱性を不正利用する条件は厳格です。攻撃者は、直接接続されたデバイスを完全に制御できる必要があります。Cisco IOS XRデバイスでは、影響はUDLDプロセスのリロードに限定されます。

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-nxos-xr-udld-dos-W5hGHgtQ

このアドバイザリは、Cisco IOSおよびIOS XEソフトウェアのセキュリティアドバイザリバンドル公開の2021年9月リリースの一部です。アドバイザリとリンクの一覧については、『

Cisco Event Response: September 2021 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

この脆弱性は、次のシスコソフトウェアの脆弱性のあるリリースを実行しているシスコデバイスに影響を与えました。 UDLD機能が有効になっているか。

- IOSソフトウェア(CSCvw46194)
- IOS XEソフトウェア(CSCvw46194)
- IOS XRソフトウェア(CSCvw46239)

この脆弱性は、公開時点で、Cisco FXOSまたはNX-OSソフトウェアの脆弱性が存在するリリースを実行し、UDLD機能が有効になっている次のシスコ製品にも影響を与えました。

- Firepower 4100シリーズ(CSCvw26130)[1]
- Firepower 9300セキュリティアプライアンス(CSCvw26130)[1]
- MDS 9000シリーズマルチレイヤスイッチ(CSCvw26126)
- Nexus 3000シリーズスイッチ(CSCvw22670)
- Nexus 5500プラットフォームスイッチ(CSCvw26127)
- Nexus 5600プラットフォームスイッチ(CSCvw26127)
- Nexus 6000シリーズスイッチ(CSCvw26127)
- Nexus 7000シリーズスイッチ(CSCvw26126)
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ(CSCvw22670)
- UCS 6200シリーズファブリックインターコネクト(CSCvw26129)
- UCS 6300シリーズファブリックインターコネクト(CSCvw26129)
- UCS 6400シリーズファブリックインターコネクト(CSCvw26152)

1. Firepower 4100および9300製品は正式にはUDLDをサポートしていませんが、CLIにはUDLDを有効にするコマンドが含まれています。これらの製品は、UDLDが誤ってイネーブルにされた場合にのみ脆弱になる可能性があります。このような場合は、UDLDをディセーブルにして、この脆弱性の影響を完全に排除することを推奨いたします。

脆弱性が存在する Cisco ソフトウェア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」セクションを参照してください。

UDLD機能のステータスの確認

デバイスでUDLD機能が有効になっているかどうかを確認するには、次の製品固有の手順に従ってください。

Cisco FXOSソフトウェアおよびUCSファブリックインターコネクト

デバイスのCLIでscope orgコマンドに続けてshow udld-link-policyコマンドを使用します。コマンド出力のAdmin Stateの下に、デフォルトおよび手動で設定されたUDLDリンクポリシーに対してEnabledまたはDisabledが表示されます。次の例は、UDLDが無効になっているデバイスでのコマンド出力を示しています。

<#root>

```
fxos#
scope org

fxos#
show udld-link-policy

UDLD link policy:
Name       Admin State UDLD mode
---------- ----------- ---------
default
Disabled
    Normal
```

Cisco IOS および IOS XE ソフトウェア

show udld | include "state: Enabled"コマンドをデバイスのCLIで実行します。コマンドの出力が返された場合は、デバイスの一部のインターフェイスでUDLD機能が設定されています。次の例は、UDLDが有効になっているデバイスでのコマンド出力を示しています。

<#root>

```
Router#
show udld | include "state: Enabled"

Port enable operational state: Enabled / in aggressive mode
```

Cisco IOS XR ソフトウェア

デバイスのCLIでshow ethernet udld interfaces briefコマンドを使用します。コマンドの出力が返された場合は、デバイスの一部のインターフェイスでUDLD機能が設定されています。次の例は、UDLDが有効になっているデバイスでのコマンド出力を示しています。

<#root>

```
RP/0/RSP0/CPU0:router#
show ethernet udld interfaces brief


Port            State          Neighbor Device                 N'bor port
  -------------  -------------- ------------------------------ -------------
  Gi0/1/0/1      Bidirectional  london-xr22.cisco.com           Gi3/12/0/24
  Gi0/1/0/2      Bidirectional  [2 neighbors]                   -
  Gi0/1/0/3      Unknown        -                               -
  Gi0/1/0/4      Unidirectional sj-ios25.cisco.com              Gi3/5
  Te0/12/0/10    Admin Down     -                               -
  Te0/12/0/11    N'bor Mismatch long-device.cisco.com           LongPortNam>>
```

Cisco NX-OS ソフトウェア

適用されたコマンドとマクロ名を表示するには、show running-config | include "feature udld" コマンドをデバイスのCLIで実行します。コマンドの出力が返された場合は、デバイスでUDLD機能が設定されています。次の例は、UDLDが有効になっているデバイスでのコマンド出力を示しています。

```
<#root>
nxos#
show running-config | include "feature udld"

feature udld
```

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、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Meraki 製品
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 9000 シリーズ ファブリック スイッチ (アプリケーション セントリック インフラ

ストラクチャ（ACI）モード）

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

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 セキュリティ アドバイザリ 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アップグレード ソリューション一式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 FXOS ソフトウェア

発行時点では、次の表に記載されているリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列はシスコソフトウェアリリースを示し、右の列はリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。

Firepower 4100シリーズおよびFirepower 9300セキュリティアプライアンス

Cisco FXOS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
2.2	2.2.2.1481
2.3	2.3.1.2161
2.4	2.4.1.2731
2.6	2.6.1.2241
2.7	2.7.1.1431
2.8	2.8.1.1431
2.9	2.9.1.1351
2.10	脆弱性なし

1. Firepower 4100および9300製品は正式にはUDLDをサポートしていませんが、CLIにはUDLDを有効にするコマンドが含まれています。これらの製品は、UDLDが誤ってイネーブルにされた場合にのみ脆弱になる可能性があります。このような場合は、UDLDをディセーブルにして、この脆弱性の影響を完全に排除することを推奨いたします。

Cisco IOS および IOS XE ソフトウェア

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できるよう、シスコでは Cisco Software Checker を提供しています。このツールにより、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。

お客様は、Cisco Software Checker を使用して次の方法でアドバイザリを検索できます。

- ソフトウェアと 1 つ以上のリリースを選択します。
- 特定のリリースのリストを含む .txt ファイルをアップロードする
- show version コマンドの出力を入力する

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリ、特定のアドバイザリ、または最新の公開資料に記載されているすべてのアドバイザリが含まれるように検索をカスタマイズできます。

また、次の形式を使用して、Cisco IOS または IOS XE ソフトウェアリリース（15.1(4)M2 や 3.13.8S など）を入力することで、そのリリースがシスコ セキュリティ アドバイザリの影響を受けているかどうかを判断できます。

Check

デフォルトでは、Cisco Software Checker の結果には、Security Impact Rating（SIR）が「重大」または「高」の脆弱性だけが含まれます。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com にある Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価（Impact Rating）] の下にある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。

Cisco IOS XR ソフトウェア

発行時点では、次の表に記載されているリリース情報は正確でした。SMUのアベイラビリティを含む最新情報については、このアドバイザリの先頭にあるバグIDの「詳細」セクションを参照してください。

左の列はシスコソフトウェアリリースを示し、右の列はリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。

Cisco IOS XR ソフトウェア リリース	この脆弱性に対する最初の修正リリース
6.6	脆弱性あり。修正済みリリースに移行してください。
6.7	6.7.4

Cisco IOS XR ソフトウェア リリース	この脆弱性に対する最初の修正リリース
6.8	6.8.1
7.2	7.2.2
7.3	7.3.1, 7.3.15
7.4	7.4.1

Cisco NX-OS ソフトウェア

お客様が Cisco NX-OS ソフトウェアの脆弱性による侵害の可能性を判断できるよう、シスコでは Cisco Software Checker を提供しています。このツールにより、特定の Cisco NX-OS 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。

お客様は、Cisco Software Checker を使用して次の方法でアドバイザリを検索できます。

- ソフトウェア、プラットフォーム、および 1 つ以上のリリースを選択する
- 特定のリリースのリストを含む .txt ファイルをアップロードする
- show version コマンドの出力を入力する

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリまたは 1 つ以上の特定のアドバイザリが含まれるように検索をカスタマイズできます。

また、次のフォームを使用して、Cisco NX-OS ソフトウェアとプラットフォームを選択、およびリリースを入力することで（例：Cisco Nexus 3000 シリーズ スイッチの 7.0(3)I7(5)、ACI モードの Cisco NX-OS ソフトウェアの 14.0(1h)）、シスコ セキュリティ アドバイザリの対象となるリリースであるかを判断することもできます。

Cisco NX-OS ソフトウェア　MDS 9000 シリーズ マルチレイヤ スイッチ

Enter Version　Check

デフォルトでは、Cisco Software Checker の結果には、Security Impact Rating（SIR）が「重大」または「高」の脆弱性だけが含まれます。「中間」の SIR 脆弱性の結果を含めるには、Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価（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。

Cisco UCS ソフトウェア

発行時点では、次の表に記載されているリリース情報は正確でした。最も完全で最新の情報につ

いては、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列はシスコソフトウェアリリースを示し、右の列はリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。

UCS 6200、6300、および6400シリーズファブリックインターコネクト

Cisco UCS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
4.0 より前	修正済みリリースに移行。
4.0	4.0(4l)
4.1	4.1(2c)
4.2	脆弱性なし

関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェアリリースの決定に際してサポートが必要な場合は、以下の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco MDS シリーズ スイッチ
Vmware スイッチ向け Cisco Nexus 1000V
Cisco Nexus 3000 Series Switches
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 5600 プラットフォームスイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 9000 Series Switches
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS ソフトウェアに最適なリリースを確認するには、デバイスのリリースノートに記載されている推奨リリースに関するドキュメントを参照してください。

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

この脆弱性は、シスコの内部セキュリティテストでMarco Cassini氏によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-nxos-xr-udld-dos-W5hGHgtQ

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	2021 年 9 月 22 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。