Cisco IOS および IOS XE ソフトウェアの Cluster Management Protocol のリモート コード実行の脆弱性

アドバイザリーID : cisco-sa-20170317-cmp
初公開日 : 2017-03-17 16:00
最終更新日 : 2019-04-17 18:47
バージョン 1.8 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCvd48893
CVE-2017-3881

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 および Cisco IOS XE ソフトウェアの Cisco Cluster Management Protocol（CMP）の処理コードに脆弱性が発見されました。認証されていないリモート攻撃者が、該当デバイスをリロードさせたり、昇格された特権でコードを実行したりできる危険性があります。

Cluster Management Protocol は、クラスタ メンバー間でのシグナリングおよびコマンド プロトコルとして、Telnet を内部で利用しています。この脆弱性は次の 2 つの要因が組み合わさって発生します。

- CMP 固有 Telnet オプションの使用を（クラスタ メンバー間内部の）ローカル通信に限定できず、該当デバイスへの Telnet 接続であらゆる Telnet オプションが処理される。
- 不正な CMP 固有 Telnet オプションが不適切に処理される。

この脆弱性は、シスコ製の該当デバイスが Telnet 接続を受け付けるように設定されている場合で、かつデバイスとの Telnet セッション確立時に不正な CMP 固有 Telnet オプションが送信された場合に、悪用される危険性があります。このエクスプロイトにより、攻撃者は任意のコードを実行してデバイスの完全な制御権を取得したり、該当デバイスをリロードさせたりする可能性があります。

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-20170317-cmp

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、以下のシスコ デバイスにおいて脆弱性が存在する Cisco IOS ソフトウェア リリースを実行しており、着信 Telnet 接続を受け付けるように設定している場合です。

- Cisco Catalyst 2350-48TD-S スイッチ
- Cisco Catalyst 2350-48TD-SD スイッチ
- Cisco Catalyst 2360-48TD-S スイッチ
- Cisco Catalyst 2918-24TC-C スイッチ
- Cisco Catalyst 2918-24TT-C スイッチ
- Cisco Catalyst 2918-48TC-C スイッチ
- Cisco Catalyst 2918-48TT-C スイッチ
- Cisco Catalyst 2928-24TC-C スイッチ
- Cisco Catalyst 2960-24-S スイッチ
- Cisco Catalyst 2960-24LC-S スイッチ
- Cisco Catalyst 2960-24LT-L スイッチ
- Cisco Catalyst 2960-24PC-L スイッチ
- Cisco Catalyst 2960-24PC-S スイッチ
- Cisco Catalyst 2960-24TC-L スイッチ
- Cisco Catalyst 2960-24TC-S スイッチ
- Cisco Catalyst 2960-24TT-L スイッチ
- Cisco Catalyst 2960-48PST-L スイッチ
- Cisco Catalyst 2960-48PST-S スイッチ
- Cisco Catalyst 2960-48TC-L スイッチ
- Cisco Catalyst 2960-48TC-S スイッチ
- Cisco Catalyst 2960-48TT-L スイッチ
- Cisco Catalyst 2960-48TT-S スイッチ
- Cisco Catalyst 2960-8TC-L コンパクト スイッチ
- Cisco Catalyst 2960-8TC-S コンパクト スイッチ
- Cisco Catalyst 2960-Plus 24LC-L スイッチ
- Cisco Catalyst 2960-Plus 24LC-S スイッチ
- Cisco Catalyst 2960-Plus 24PC-L スイッチ
- Cisco Catalyst 2960-Plus 24PC-S スイッチ
- Cisco Catalyst 2960-Plus 24TC-L スイッチ
- Cisco Catalyst 2960-Plus 24TC-S スイッチ
- Cisco Catalyst 2960-Plus 48PST-L スイッチ

- Cisco Catalyst 2960-Plus 48PST-S スイッチ
- Cisco Catalyst 2960-Plus 48TC-L スイッチ
- Cisco Catalyst 2960-Plus 48TC-S スイッチ
- Cisco Catalyst 2960C-12PC-L スイッチ
- Cisco Catalyst 2960C-8PC-L スイッチ
- Cisco Catalyst 2960C-8TC-L スイッチ
- Cisco Catalyst 2960C-8TC-S スイッチ
- Cisco Catalyst 2960CG-8TC-L コンパクト スイッチ
- Cisco Catalyst 2960CPD-8PT-L スイッチ
- Cisco Catalyst 2960CPD-8TT-L スイッチ
- Cisco Catalyst 2960CX-8PC-L スイッチ
- Cisco Catalyst 2960CX-8TC-L スイッチ
- Cisco Catalyst 2960G-24TC-L スイッチ
- Cisco Catalyst 2960G-48TC-L スイッチ
- Cisco Catalyst 2960G-8TC-L コンパクト スイッチ
- Cisco Catalyst 2960L-16PS-LL スイッチ
- Cisco Catalyst 2960L-16TS-LL スイッチ
- Cisco Catalyst 2960L-24PS-LL スイッチ
- Cisco Catalyst 2960L-24TS-LL スイッチ
- Cisco Catalyst 2960L-48PS-LL スイッチ
- Cisco Catalyst 2960L-48TS-LL スイッチ
- Cisco Catalyst 2960L-8PS-LL スイッチ
- Cisco Catalyst 2960L-8TS-LL スイッチ
- Cisco Catalyst 2960PD-8TT-L コンパクト スイッチ
- Cisco Catalyst 2960S-24PD-L スイッチ
- Cisco Catalyst 2960S-24PS-L スイッチ
- Cisco Catalyst 2960S-24TD-L スイッチ
- Cisco Catalyst 2960S-24TS-L スイッチ
- Cisco Catalyst 2960S-24TS-S スイッチ
- Cisco Catalyst 2960S-48FPD-L スイッチ
- Cisco Catalyst 2960S-48FPS-L スイッチ
- Cisco Catalyst 2960S-48LPD-L スイッチ
- Cisco Catalyst 2960S-48LPS-L スイッチ
- Cisco Catalyst 2960S-48TD-L スイッチ
- Cisco Catalyst 2960S-48TS-L スイッチ
- Cisco Catalyst 2960S-48TS-S スイッチ
- Cisco Catalyst 2960S-F24PS-L スイッチ
- Cisco Catalyst 2960S-F24TS-L スイッチ
- Cisco Catalyst 2960S-F24TS-S スイッチ
- Cisco Catalyst 2960S-F48FPS-L スイッチ
- Cisco Catalyst 2960S-F48LPS-L スイッチ

- Cisco Catalyst 2960S-F48TS-L スイッチ
- Cisco Catalyst 2960S-F48TS-S スイッチ
- Cisco Catalyst 2960X-24PD-L スイッチ
- Cisco Catalyst 2960X-24PS-L スイッチ
- Cisco Catalyst 2960X-24PSQ-L クール スイッチ
- Cisco Catalyst 2960X-24TD-L スイッチ
- Cisco Catalyst 2960X-24TS-L スイッチ
- Cisco Catalyst 2960X-24TS-LL スイッチ
- Cisco Catalyst 2960X-48FPD-L スイッチ
- Cisco Catalyst 2960X-48FPS-L スイッチ
- Cisco Catalyst 2960X-48LPD-L スイッチ
- Cisco Catalyst 2960X-48LPS-L スイッチ
- Cisco Catalyst 2960X-48TD-L スイッチ
- Cisco Catalyst 2960X-48TS-L スイッチ
- Cisco Catalyst 2960X-48TS-LL スイッチ
- Cisco Catalyst 2960XR-24PD-I スイッチ
- Cisco Catalyst 2960XR-24PD-L スイッチ
- Cisco Catalyst 2960XR-24PS-I スイッチ
- Cisco Catalyst 2960XR-24PS-L スイッチ
- Cisco Catalyst 2960XR-24TD-I スイッチ
- Cisco Catalyst 2960XR-24TD-L スイッチ
- Cisco Catalyst 2960XR-24TS-I スイッチ
- Cisco Catalyst 2960XR-24TS-L スイッチ
- Cisco Catalyst 2960XR-48FPD-I スイッチ
- Cisco Catalyst 2960XR-48FPD-L スイッチ
- Cisco Catalyst 2960XR-48FPS-I スイッチ
- Cisco Catalyst 2960XR-48FPS-L スイッチ
- Cisco Catalyst 2960XR-48LPD-I スイッチ
- Cisco Catalyst 2960XR-48LPD-L スイッチ
- Cisco Catalyst 2960XR-48LPS-I スイッチ
- Cisco Catalyst 2960XR-48LPS-L スイッチ
- Cisco Catalyst 2960XR-48TD-I スイッチ
- Cisco Catalyst 2960XR-48TD-L スイッチ
- Cisco Catalyst 2960XR-48TS-I スイッチ
- Cisco Catalyst 2960XR-48TS-L スイッチ
- Cisco Catalyst 2970G-24T スイッチ
- Cisco Catalyst 2970G-24TS スイッチ
- Cisco Catalyst 2975 スイッチ
- Cisco Catalyst 3550 12G スイッチ
- Cisco Catalyst 3550 12T スイッチ
- Cisco Catalyst 3550 24 DC SMI スイッチ

- Cisco Catalyst 3550 24 EMI スイッチ
- Cisco Catalyst 3550 24 FX SMI スイッチ
- Cisco Catalyst 3550 24 PWR スイッチ
- Cisco Catalyst 3550 24 SMI スイッチ
- Cisco Catalyst 3550 48 EMI スイッチ
- Cisco Catalyst 3550 48 SMI スイッチ
- Cisco Catalyst 3560-12PC-S コンパクト スイッチ
- Cisco Catalyst 3560-24PS スイッチ
- Cisco Catalyst 3560-24TS スイッチ
- Cisco Catalyst 3560-48PS スイッチ
- Cisco Catalyst 3560-48TS スイッチ
- Cisco Catalyst 3560-8PC コンパクト スイッチ
- Cisco Catalyst 3560C-12PC-S スイッチ
- Cisco Catalyst 3560C-8PC-S スイッチ
- Cisco Catalyst 3560CG-8PC-S コンパクト スイッチ
- Cisco Catalyst 3560CG-8TC-S コンパクト スイッチ
- Cisco Catalyst 3560CPD-8PT-S コンパクト スイッチ
- Cisco Catalyst 3560CX-12PC-S スイッチ
- Cisco Catalyst 3560CX-12PD-S スイッチ
- Cisco Catalyst 3560CX-12TC-S スイッチ
- Cisco Catalyst 3560CX-8PC-S スイッチ
- Cisco Catalyst 3560CX-8PT-S スイッチ
- Cisco Catalyst 3560CX-8TC-S スイッチ
- Cisco Catalyst 3560CX-8XPD-S スイッチ
- Cisco Catalyst 3560E-12D-E スイッチ
- Cisco Catalyst 3560E-12D-S スイッチ
- Cisco Catalyst 3560E-12SD-E スイッチ
- Cisco Catalyst 3560E-12SD-S スイッチ
- Cisco Catalyst 3560E-24PD-E スイッチ
- Cisco Catalyst 3560E-24PD-S スイッチ
- Cisco Catalyst 3560E-24TD-E スイッチ
- Cisco Catalyst 3560E-24TD-S スイッチ
- Cisco Catalyst 3560E-48PD-E スイッチ
- Cisco Catalyst 3560E-48PD-EF スイッチ
- Cisco Catalyst 3560E-48PD-S スイッチ
- Cisco Catalyst 3560E-48PD-SF スイッチ
- Cisco Catalyst 3560E-48TD-E スイッチ
- Cisco Catalyst 3560E-48TD-S スイッチ
- Cisco Catalyst 3560G-24PS スイッチ
- Cisco Catalyst 3560G-24TS スイッチ
- Cisco Catalyst 3560G-48PS スイッチ

- Cisco Catalyst 3560G-48TS スイッチ
- Cisco Catalyst 3560V2-24DC スイッチ
- Cisco Catalyst 3560V2-24PS スイッチ
- Cisco Catalyst 3560V2-24TS スイッチ
- Cisco Catalyst 3560V2-48PS スイッチ
- Cisco Catalyst 3560V2-48TS スイッチ
- Cisco Catalyst 3560X-24P-E スイッチ
- Cisco Catalyst 3560X-24P-L スイッチ
- Cisco Catalyst 3560X-24P-S スイッチ
- Cisco Catalyst 3560X-24T-E スイッチ
- Cisco Catalyst 3560X-24T-L スイッチ
- Cisco Catalyst 3560X-24T-S スイッチ
- Cisco Catalyst 3560X-24U-E スイッチ
- Cisco Catalyst 3560X-24U-L スイッチ
- Cisco Catalyst 3560X-24U-S スイッチ
- Cisco Catalyst 3560X-48P-E スイッチ
- Cisco Catalyst 3560X-48P-L スイッチ
- Cisco Catalyst 3560X-48P-S スイッチ
- Cisco Catalyst 3560X-48PF-E スイッチ
- Cisco Catalyst 3560X-48PF-L スイッチ
- Cisco Catalyst 3560X-48PF-S スイッチ
- Cisco Catalyst 3560X-48T-E スイッチ
- Cisco Catalyst 3560X-48T-L スイッチ
- Cisco Catalyst 3560X-48T-S スイッチ
- Cisco Catalyst 3560X-48U-E スイッチ
- Cisco Catalyst 3560X-48U-L スイッチ
- Cisco Catalyst 3560X-48U-S スイッチ
- Cisco Catalyst 3750 Metro 24-AC スイッチ
- Cisco Catalyst 3750 Metro 24-DC スイッチ
- Cisco Catalyst 3750-24FS スイッチ
- Cisco Catalyst 3750-24PS スイッチ
- Cisco Catalyst 3750-24TS スイッチ
- Cisco Catalyst 3750-48PS スイッチ
- Cisco Catalyst 3750-48TS スイッチ
- Cisco Catalyst 3750E-24PD-E スイッチ
- Cisco Catalyst 3750E-24PD-S スイッチ
- Cisco Catalyst 3750E-24TD-E スイッチ
- Cisco Catalyst 3750E-24TD-S スイッチ
- Cisco Catalyst 3750E-48PD-E スイッチ
- Cisco Catalyst 3750E-48PD-EF スイッチ
- Cisco Catalyst 3750E-48PD-S スイッチ

- Cisco Catalyst 3750E-48PD-SF スイッチ
- Cisco Catalyst 3750E-48TD-E スイッチ
- Cisco Catalyst 3750E-48TD-S スイッチ
- Cisco Catalyst 3750G-12S スイッチ
- Cisco Catalyst 3750G-12S-SD スイッチ
- Cisco Catalyst 3750G-16TD スイッチ
- Cisco Catalyst 3750G-24PS スイッチ
- Cisco Catalyst 3750G-24T スイッチ
- Cisco Catalyst 3750G-24TS スイッチ
- Cisco Catalyst 3750G-24TS-1U スイッチ
- Cisco Catalyst 3750G-48PS スイッチ
- Cisco Catalyst 3750G-48TS スイッチ
- Cisco Catalyst 3750V2-24FS スイッチ
- Cisco Catalyst 3750V2-24PS スイッチ
- Cisco Catalyst 3750V2-24TS スイッチ
- Cisco Catalyst 3750V2-48PS スイッチ
- Cisco Catalyst 3750V2-48TS スイッチ
- Cisco Catalyst 3750X-12S-E スイッチ
- Cisco Catalyst 3750X-12S-S スイッチ
- Cisco Catalyst 3750X-24P-E スイッチ
- Cisco Catalyst 3750X-24P-L スイッチ
- Cisco Catalyst 3750X-24P-S スイッチ
- Cisco Catalyst 3750X-24S-E スイッチ
- Cisco Catalyst 3750X-24S-S スイッチ
- Cisco Catalyst 3750X-24T-E スイッチ
- Cisco Catalyst 3750X-24T-L スイッチ
- Cisco Catalyst 3750X-24T-S スイッチ
- Cisco Catalyst 3750X-24U-E スイッチ
- Cisco Catalyst 3750X-24U-L スイッチ
- Cisco Catalyst 3750X-24U-S スイッチ
- Cisco Catalyst 3750X-48P-E スイッチ
- Cisco Catalyst 3750X-48P-L スイッチ
- Cisco Catalyst 3750X-48P-S スイッチ
- Cisco Catalyst 3750X-48PF-E スイッチ
- Cisco Catalyst 3750X-48PF-L スイッチ
- Cisco Catalyst 3750X-48PF-S スイッチ
- Cisco Catalyst 3750X-48T-E スイッチ
- Cisco Catalyst 3750X-48T-L スイッチ
- Cisco Catalyst 3750X-48T-S スイッチ
- Cisco Catalyst 3750X-48U-E スイッチ
- Cisco Catalyst 3750X-48U-L スイッチ

- Cisco Catalyst 3750X-48U-S スイッチ
- Cisco Catalyst 4000 Supervisor Engine I
- Cisco Catalyst 4000/4500 Supervisor Engine IV
- Cisco Catalyst 4000/4500 Supervisor Engine V
- Cisco Catalyst 4500 シリーズ Supervisor Engine II-Plus
- Cisco Catalyst 4500 シリーズ Supervisor Engine II-Plus-TS
- Cisco Catalyst 4500 シリーズ Supervisor Engine V-10GE
- Cisco Catalyst 4500 シリーズ Supervisor II-Plus-10GE
- Cisco Catalyst 4500 Supervisor Engine 6-E
- Cisco Catalyst 4500 Supervisor Engine 6L-E
- Cisco Catalyst 4500E Supervisor Engine 8-E
- Cisco Catalyst 4900M スイッチ
- Cisco Catalyst 4928 10 ギガビット イーサネット スイッチ
- Cisco Catalyst 4948 10 ギガビット イーサネット スイッチ
- Cisco Catalyst 4948 スイッチ
- Cisco Catalyst 4948E イーサネット スイッチ
- Cisco Catalyst 4948E-F イーサネット スイッチ
- Cisco Catalyst Blade Switch 3020 for HP
- Cisco Catalyst Blade Switch 3030 for Dell
- Cisco Catalyst Blade Switch 3032 for Dell M1000E
- Cisco Catalyst Blade Switch 3040 for FSC
- Cisco Catalyst Blade Switch 3120 for HP
- Cisco Catalyst Blade Switch 3120X for HP
- Cisco Catalyst Blade Switch 3130 for Dell M1000E
- Cisco Catalyst C2928-24LT-C スイッチ
- Cisco Catalyst C2928-48TC-C スイッチ
- Cisco Catalyst Switch Module 3012 for IBM BladeCenter
- Cisco Catalyst Switch Module 3110 for IBM BladeCenter
- Cisco Catalyst Switch Module 3110X for IBM BladeCenter
- Cisco Embedded Service 2020 24TC CON B スイッチ
- Cisco Embedded Service 2020 24TC CON スイッチ
- Cisco Embedded Service 2020 24TC NCP B スイッチ
- Cisco Embedded Service 2020 24TC NCP スイッチ
- Cisco Embedded Service 2020 CON B スイッチ
- Cisco Embedded Service 2020 CON スイッチ
- Cisco Embedded Service 2020 NCP B スイッチ
- Cisco Embedded Service 2020 NCP スイッチ
- Cisco Enhanced Layer 2 EtherSwitch サービス モジュール
- Cisco Enhanced Layer 2/3 EtherSwitch サービス モジュール
- Cisco Gigabit Ethernet Switch Module（CGESM）for HP
- Cisco IE 2000-16PTC-G 産業用イーサネット スイッチ

- Cisco IE 2000-16T67 産業用イーサネット スイッチ
- Cisco IE 2000-16T67P 産業用イーサネット スイッチ
- Cisco IE 2000-16TC 産業用イーサネット スイッチ
- Cisco IE 2000-16TC-G 産業用イーサネット スイッチ
- Cisco IE 2000-16TC-G-E 産業用イーサネット スイッチ
- Cisco IE 2000-16TC-G-N 産業用イーサネット スイッチ
- Cisco IE 2000-16TC-G-X 産業用イーサネット スイッチ
- Cisco IE 2000-24T67 産業用イーサネット スイッチ
- Cisco IE 2000-4S-TS-G 産業用イーサネット スイッチ
- Cisco IE 2000-4T 産業用イーサネット スイッチ
- Cisco IE 2000-4T-G 産業用イーサネット スイッチ
- Cisco IE 2000-4TS 産業用イーサネット スイッチ
- Cisco IE 2000-4TS-G 産業用イーサネット スイッチ
- Cisco IE 2000-8T67 産業用イーサネット スイッチ
- Cisco IE 2000-8T67P 産業用イーサネット スイッチ
- Cisco IE 2000-8TC 産業用イーサネット スイッチ
- Cisco IE 2000-8TC-G 産業用イーサネット スイッチ
- Cisco IE 2000-8TC-G-E 産業用イーサネット スイッチ
- Cisco IE 2000-8TC-G-N 産業用イーサネット スイッチ
- Cisco IE 3000-4TC 産業用イーサネット スイッチ
- Cisco IE 3000-8TC 産業用イーサネット スイッチ
- Cisco IE-3010-16S-8PC 産業用イーサネット スイッチ
- Cisco IE-3010-24TC 産業用イーサネット スイッチ
- Cisco IE-4000-16GT4G-E 産業用イーサネット スイッチ
- Cisco IE-4000-16T4G-E 産業用イーサネット スイッチ
- Cisco IE-4000-4GC4GP4G-E 産業用イーサネット スイッチ
- Cisco IE-4000-4GS8GP4G-E 産業用イーサネット スイッチ
- Cisco IE-4000-4S8P4G-E 産業用イーサネット スイッチ
- Cisco IE-4000-4T4P4G-E 産業用イーサネット スイッチ
- Cisco IE-4000-4TC4G-E 産業用イーサネット スイッチ
- Cisco IE-4000-8GS4G-E 産業用イーサネット スイッチ
- Cisco IE-4000-8GT4G-E 産業用イーサネット スイッチ
- Cisco IE-4000-8GT8GP4G-E 産業用イーサネット スイッチ
- Cisco IE-4000-8S4G-E 産業用イーサネット スイッチ
- Cisco IE-4000-8T4G-E 産業用イーサネット スイッチ
- Cisco IE-4010-16S12P 産業用イーサネット スイッチ
- Cisco IE-4010-4S24P 産業用イーサネット スイッチ
- Cisco IE-5000-12S12P-10G 産業用イーサネット スイッチ
- Cisco IE-5000-16S12P 産業用イーサネット スイッチ
- Cisco ME 4924-10GE スイッチ
- Cisco RF ゲートウェイ 10

- Cisco SM-X レイヤ 2/3 EtherSwitch サービス モジュール

注：CMP サブシステムの存在を確認する必要があるのは、Cisco IOS ソフトウェアではなく、Cisco IOS XE ソフトウェアが実行されているデバイスのみです。デバイスが Telnet 接続を受け付けるように設定されているかどうかを確認するには、Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアを実行しているデバイスが必要になります。

脆弱性が存在する Cisco IOS XE リリースを実行しているシスコ デバイスでは、以下の条件が満たされた場合に、この脆弱性の影響を受けます。

- デバイス上で実行している Cisco IOS XE ソフトウェア イメージに CMP サブシステムが存在する。
- デバイスが着信 Telnet 接続を受け付けるように設定されている。

CMP サブシステムが、実行中のソフトウェア イメージに存在しているかどうかを判断するには、デバイスの特権 CLI プロンプトで show subsys class protocol | include ^cmp コマンドを実行します。

次の例は、デバイスで実行中のソフトウェア イメージに CMP サブシステムが存在していない場合の、 show subsys class protocol | include ^cmp コマンドの出力結果を示します。

```
Switch#show subsys class protocol | include ^cmp
cmp                                  Protocol    1.000.001
Switch#
```

次の例は、デバイスで実行中のソフトウェア イメージに CMP サブシステムが存在していない場合の、 show subsys class protocol | include ^cmp コマンドの出力結果を示します。

```
Switch#show subsys class protocol | include ^cmp
Switch#
```

デバイスが Telnet 接続の受信を承認するように設定されているかどうかを判断するには、特権 CLI プロンプトで show running-config | include ^line vty|transport inputコマンドを実行します。コマンド出力では、以下のような設定が表示されます。

- line vty 設定行の後に transport input 設定行がない場合、デバイスでは、仮想端末（VTY）経由の着信接続にデフォルトのプロトコル セットを使用しています。デフォルトのプロトコル セットには Telnet プロトコルが含まれているため、このデバイスはすべ

ての VTY で Telnet 接続を受け付けます。この設定では脆弱性の影響を受けます。

```
Switch#show running-config | include ^line vty|transport input
line vty 0 4
line vty 5 15
Switch#
```

- このデバイスでは、一部の VTY への着信接続については、Secure Shell (SSH) プロトコルのみを受け付けるように明示的に設定されていますが、6 ~ 15 の VTY はデフォルトのプロトコル セットを使用しています。従って、それらの VTY への Telnet 接続は受け付けられます。この設定では脆弱性の影響を受けます。

```
Switch#show running-config | include ^line vty|transport input
line vty 0 4
 transport input ssh
line vty 5
 transport input ssh
line vty 6 15
Switch#
```

- すべての VTY への着信接続について、利用可能なすべての転送プロトコルが有効になっています。すべてのプロトコルを有効にすると Telnet プロトコルも有効になるため、デバイスへの Telnet 接続が可能になります。この設定では脆弱性の影響を受けます。

```
Switch#show running-config | include ^line vty|transport input
line vty 0 4
 transport input all
line vty 5 15
 transport input all
Switch#
```

- すべての VTY の着信接続について、SSH プロトコルのみが有効になっています。この設定を使用している場合、デバイスの VTY への Telnet 接続は不可能です。この設定は脆弱性の影響を受けません。

```
Switch#show running-config | include ^line vty|transport input
line vty 0 4
 transport input ssh
line vty 5 15
 transport input ssh
Switch#
```

- すべての VTY の着信接続で許可されるプロトコルとして、Telnet と SSH プロトコルの両方が明示的に有効になっています。この設定では、デバイスへの Telnet 接続が成功します。この設定では脆弱性の影響を受けます。

```
Switch#show running-config | include ^line vty|transport input
line vty 0 4
 transport input telnet ssh
line vty 5 15
 transport input telnet ssh
```

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、『White Paper: 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、『White Paper: 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

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。

脆弱性が存在する Cisco IOS ソフトウェア リリースを実行しているが、本アドバイザリの「脆弱性が存在する製品」セクションに記載されていないシスコ デバイスについては、この脆弱性の影響を受けません。

脆弱性が存在する Cisco IOS XE ソフトウェア リリースを実行しているが、CMP プロトコル サブシステムを含んでいないシスコ デバイスについては、この脆弱性の影響を受けません。

詳細

Cisco IOS および Cisco IOS XE ソフトウェアの Cisco Cluster Management Protocol（CMP）の処理コードに脆弱性が発見されました。認証されていないリモート攻撃者が、該当デバイスをリ

ロードさせたり、昇格された特権でコードを実行したりできる危険性があります。

Cluster Management Protocol は、クラスタ メンバー間でのシグナリングおよびコマンド プロトコルとして、Telnet を内部で利用しています。この脆弱性は次の 2 つの要因が組み合わさって発生します。

- CMP 固有 Telnet オプションの使用を（クラスタ メンバー間内部の）ローカル通信に限定できず、該当デバイスへの Telnet 接続であらゆる Telnet オプションが処理される。
- 不正な CMP 固有 Telnet オプションが不適切に処理される。

この脆弱性は、シスコ製の該当デバイスが Telnet 接続を受け付けるように設定されている場合で、かつデバイスとの Telnet セッション確立時に不正な CMP 固有 Telnet オプションが送信された場合に、悪用される危険性があります。このエクスプロイトにより、攻撃者は任意のコードを実行してデバイスの完全な制御権を取得したり、該当デバイスをリロードさせたりする可能性があります。

デバイス設定にクラスタ設定コマンドが存在しない場合でも、CMP 固有の Telnet オプションはデフォルトで処理されます。

この脆弱性は、IPv4 または IPv6 での Telnet セッション ネゴシエーション中に不正利用されます。この脆弱性が不正利用されるのは、デバイスに対して確立された Telnet セッションのみです。デバイスを経由する Telnet セッションで不正なオプションを送信しても、この脆弱性は引き起こされません。

セキュリティ侵害の痕跡

Cisco IPS シグネチャ 7880-0 および Snort SID 41909 および 41910 はこの脆弱性を不正利用する試みを検出します。

回避策

この脆弱性に対処する回避策はありません。

着信接続で許可されるプロトコルとして Telnet プロトコルを無効にすれば、この不正利用手段を排除できます。シスコは Telnet の無効化と SSH の使用を推奨します。両方の設定方法については、『Cisco IOS デバイスのセキュリティ強化に関するガイド』を参照してください。

Telnet プロトコルを無効にできない、または無効にしたくない場合は、VTY アクセス リスト（デバイス レベルで）またはインフラストラクチャ アクセス コントロール リスト（iACL）を導入すると、攻撃対象領域を削減できます。VTY アクセスリストの詳細については、 Cisco Guide to Harden Cisco IOS Devices を参照してください。iACL の詳細については、 Protecting Your Core: Infrastructure Protection Access Control Lists を参照してください。

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リリースしています。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、アクセスまたはその他の方法で使用した場合、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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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、[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は新規リリースでも継続して適切なサポートが受けられることを確認してください。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 Cisco Service Contract 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 POS 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。
http://www.cisco.com/c/ja_jp/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。

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 メニューからリリース（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

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、Cisco IOS XE ソフトウェアのリリースに応じて「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、または「Cisco IOS XE 3SG Release Notes」を参照してください。

不正利用事例と公式発表

このアドバイザリで説明された脆弱性に対するエクスプロイト コードは、2017 年 4 月 10 日にセキュリティ研究者が提供しました。

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がすでにエクスプロイトされていることを認識しています。追加情報については、『Cisco TALOS：インターネットの中核技術への信頼性を悪用する DNS ハイジャック』を参照してください。

出典

この脆弱性は、Vault 7 の公開に関連した文書分析で発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.8	「エクスプロイト事例やその公表」に、確認済みの最新エクスプロイト事例を追加。	不正利用事例と公式発表	Final	2019 年 4 月 17 日
1.7	Cisco Catalyst 4500E Supervisor Engine 8-E を含めるように、脆弱性のある製品のセクションを更新。	脆弱性が存在する製品	Final	2018 年 3 月 6 日
1.6	このアドバイザリにリンクされている Common Vulnerability Reporting Framework（CVRF）ファイルを更新。	アドバイザリ ヘッダ	Final	2017 年 9 月 21 日
1.5	このアドバイザリにリンクされている Common Vulnerability Reporting Framework（CVRF）ファイルを更新。	アドバイザリ ヘッダ	Final	2017 年 9 月 19 日
1.4	修正済みソフトウェアの入手に関する情報を更新	概要および修正済みソフトウェア	Final	2017 年 5 月 8 日
1.3	このアドバイザリで説明している脆弱性のエクスプロイトの一般入手性の情報を追加。	不正利用事例と公式発表	Final	2017 年 4 月 13 日
1.2	OVAL の定義を追加。アドバイザリの内容は変更されていません。	アドバイザリ ヘッダ	Final	2017 年 4 月 3 日
1.1	VTY アクセス リストに関する情報を追加。	回避策	Final	2017 年 3 月 29 日
1.0	初回公開リリース	—	Final	2017 年 3 月 17 日

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。