Cisco IOS および IOS XE ソフトウェア Cluster Management Protocol リモート コード 実行脆弱性

Critical

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 : 2017-09-21 14:39

バージョン 1.6 : 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 のコードおよび Cisco IOS XE ソフトウェアを処理する Cisco Cluster Management Protocol （ CMP ）の脆弱性により非認証、リモート攻撃者が影響を受けたデバイスのリロードを引き起こすか、またはリモートで高度な特権のコードを実行することを可能にする可能性があります。

Cluster Management Protocol はクラスタ メンバー間のシグナリングおよびコマンド プロトコルとして Telnet を内部で利用します。 脆弱性は 2 つのファクタの組み合せが原因です:

- CMP 仕様 Telnetオプションの使用をクラスタ メンバー間の内部、ローカル通信にだけ制限し、代りに影響を受けたデバイスに Telnet接続上のそのようなオプションを受け入れ、処理する失敗
- 形式が間違った CMP 仕様 Telnetオプションの不正確な処理。

攻撃者は形式が間違った CMP 仕様 Telnetオプションの送信によって Telnet接続を許可するために影響を受けた Ciscoデバイスが設定されている Telnetセッションを設定している間この脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者が任意のコードを実行し、デバイスの完全な制御を得るか、または影響を受けたデバイスのリロードを引き起こすことを可能にする可能性があります。

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-20170317-cmp

該当製品

脆弱性のある製品

この脆弱性は脆弱な Cisco IOS ソフトウェア リリースを実行するとき着信Telnet 接続を許可するために設定される次の Ciscoデバイスに影響を与え、:

- 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 スーパバイザ エンジン II-Plus-TS

- Cisco Catalyst 4500 シリーズ Supervisor Engine V-10GE
- Cisco Catalyst 4500 シリーズ スーパバイザ II-Plus-10GE
- Cisco Catalyst 4500 Supervisor Engine 6-E
- Cisco Catalyst 4500 スーパバイザ エンジン 6L-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
- HP のための Cisco Catalyst ブレード スイッチ 3120X
- 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
- IBM BladeCenter のための Cisco Catalyst スイッチ モジュール 3110X
- 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 Service Module
- Cisco Gigabit Ethernet Switch Module（CGESM）for HP （CGESM） HP のために
- 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: 実行するデバイス Cisco IOS XE ソフトウェアだけで CMP サブシステムの存在があるように確認が、ない Cisco IOSソフトウェア必要となります。 Telnet接続を許可するためにデバイスが設定されるかどうか実行するデバイス Cisco IOS か Cisco IOS XE ソフトウェアに確認することが必要となります。

脆弱な Cisco IOS XE リリースを実行する Ciscoデバイスはこの脆弱性から次の条件が満たされるとき影響を受けます:

- CMP サブシステムはデバイスで動作する Cisco IOS XE ソフトウェア イメージにあります
- デバイスは着信Telnet 接続を許可するために設定されます。

CMP サブシステムが実行ソフトウェア イメージにあったかどうか確認するために、コマンドを **示しますサブシステム クラス プロトコルを**実行して下さい **|** デバイスの特権 CLI プロンプトからの **^cmp を含んで下さい**。

次の例はコマンドの出力が **サブシステム クラス プロトコルを示すことを**示します **|** CMP サブシステムがデバイスで動作するソフトウェア イメージに時 **^cmp を含んで下さい**:

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

次の例はコマンドの出力が **サブシステム クラス プロトコルを示すことを**示します **|** CMP サブシステムがデバイスで動作するソフトウェア イメージに時 **^cmp を含んで下さい**:

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

着信Telnet 接続を許可するためにデバイスが設定されたかどうか確認するためにコマンド **show running-config を**実行して下さい **| ^line VTY を含んで下さい|**特権 CLI プロンプトからの **トランスポート入力**。 コマンド 出力は次のような複数の可能性のある設定の 1 つを、示すかもしれません:

- *行 VTY* 設定行がデバイスを示した後*トランスポート入力* 設定行の不在は仮想端末装置（VTY）を通して着信接続のためにプロトコルの既定のセットを使用しています。 プロトコルの既定のセットは Telnet プロトコルが含まれています; それ故に、このデバイスはすべての VTY の Telnet接続を許可します。 これは脆弱な設定です。

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

- デバイスは明示的に*利用可能な* VTY *のサブセット*に着信接続のためのセキュア シェル（SSH）プロトコルを受け入れるためにただ設定されましたが番号が付いている VTY は 6 から 15 まだプロトコルの既定のセットを使用しています。 それ故に、このデバイスはそれらの VTY に Telnet接続を許可します。 これは脆弱な設定です。

```
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#
```

- すべての利用可能な転送 プロトコルはすべての VTY への着信接続のためにイネーブルになっていました。 すべてのプロトコルをイネーブルにすることはまた Telnet プロトコルを有効に し、デバイスに Telnet接続を可能にします。 これは脆弱な設定です。

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

- SSH プロトコルはすべての VTY の着信接続のためにイネーブルになっている唯一のプロトコルです。 Telnet接続はこの設定を使用しながらデバイスのあらゆる VTY に可能性のあるではないです。 この設定は脆弱ではないです。

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

- Telnet および SSH プロトコルは両方すべての VTY の着信接続のための許可されたプロトコルとして明示的にイネーブルになっていました。 デバイスへの Telnet接続はこの設定の下で正常です。 これは脆弱な設定です。

```
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ます

。その後ろには Cisco IOS ソフトウェアのリリース番号とリリース名も表示されます。 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することがあります。

次の例は Cisco IOS ソフトウェア リリース 15.5(2)T1 を実行して、*C2951-UNIVERSALK9-M* のインストール済みイメージ名前があるデバイスのためのコマンドの出力を示したものです:

```
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ついては、以下を参照してください。[ホワイト ペーパー： Cisco IOS および NX-OS ソフトウェア リファレンス ガイド]

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する場合、システム バナーは *Cisco IOSソフトウェア*、*Cisco IOS XE ソフトウェア*、または同じようなテキストを表示します。

次の例は Cisco IOS XE ソフトウェア リリース 16.2.1 を実行して、*CAT3K_CAA-UNIVERSALK9-M* のインストール済みイメージ名前があるデバイスのためのコマンドの出力を示したものです:

```
ios-xe-device# show version

Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali
16.2.1, RELEASE SOFTWARE (fc1)
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ついては、以下を参照してください。[ホワイト ペーパー： Cisco IOS および NX-OS ソフトウェア リファレンス ガイド]

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。

Cisco IOS

CMP プロトコル サブシステムを含む脆弱な Cisco IOS XE ソフトウェア リリースをしかしない実行する Ciscoデバイスはこの脆弱性から影響を受けません。

詳細

Cisco IOS のコードおよび Cisco IOS XE ソフトウェアを処理する Cisco Cluster Management Protocol（CMP）の脆弱性により非認証、リモート攻撃者が影響を受けたデバイスのリロードを引き起こすか、またはリモートで高度な特権のコードを実行することを可能にする可能性があります。

Cluster Management Protocol はクラスタ メンバー間のシグナリングおよびコマンド プロトコルとして Telnet を内部で利用します。 脆弱性は 2 つのファクタの組み合せが原因です:

- CMP 仕様 Telnetオプションの使用をクラスタ メンバー間の内部、ローカル通信にだけ制限し、代りに影響を受けたデバイスに Telnet接続上のそのようなオプションを受け入れ、処理する失敗
- 形式が間違った CMP 仕様 Telnetオプションの不正確な処理。

攻撃者は形式が間違った CMP 仕様 Telnetオプションの送信によって Telnet接続を許可するために影響を受けた Ciscoデバイスが設定されている Telnetセッションを設定している間この脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者が任意のコードを実行し、デバイスの完全な制御を得るか、または影響を受けたデバイスのリロードを引き起こすことを可能にする可能性があります。

CMP 仕様 Telnetオプションはクラスタ設定コマンドがデバイスコンフィギュレーションになくても、デフォルトで処理されます。

この脆弱性は IPv4 または IPv6 上の Telnetセッション ネゴシエーションの間に不正利用することができます。 この脆弱性はデバイスに設定される Telnetセッションを通してしか不正利用することができません—デバイスを通した Telnetセッションの形式が間違ったオプションを送信 することは脆弱性を誘発しません。

セキュリティ侵害の痕跡

Cisco IPS シグニチャ 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できます。

回避策

この脆弱性に対処する回避策はありません。

着信接続のための許可されたプロトコルとして Telnet プロトコルをディセーブルにすることはエクスプロイト ベクトルを除去します。 Telnet をディセーブルにし、SSH を使用することは Cisco によって推奨されます。 方法の情報は Cisco ガイドで両方をする Cisco IOSデバイスを堅くすると見つけることができます。

Telnet プロトコルを無効に することが不可能なか不本意顧客は 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 アクセス制御アクセス・コントロール・リスト（iACLs）の設定によって不正侵入サーフェイスを減らすことができます。 VTY アクセス リストの情報は文書で見つけることができます: Cisco IOSデバイスを堅くする Cisco ガイド。 iACLs の情報は文書で見つけることができます: **コアの保護：** インフラストラクチャ保護 ACL』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。
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、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。

http://www.cisco.com/en/US/support/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

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 IOS Software Checker ツールを提供しています。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、すべてのアドバイザリに記載されたすべて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含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全アドバイザリを含めるなど）を作成する

リリースがあらゆる公開された Cisco Security Advisory から影響を受けするかどうか判別するために、Cisco.com の Cisco IOSソフトウェア チェッカーを使用するか、または—次のフィールドで… Cisco IOSソフトウェアまたは Cisco IOS XE ソフトウェア リリースを—たとえば、**15.1(4)M2** か **3.13.8S** 入力して下さい:

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 アドバイザリに記載される 脆弱性のためのエクスプロイト コードはセキュリティ研究者によって使用できるように 2017 年 4月 10 日されました。

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のエクスプロイト事例は確認していません。

出典

この脆弱性は地下 7 公開に関した文書の分析の間に発見されました。

URL

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

改訂履歴

Version	Description	Section	Status	日付
1.6	この状況報告にリンクされるよくある脆弱性レポート フレームワーク（CVRF）ファイルをアップデートしました。	諮問ヘッダ	Final	2017 年 9 月 21 日
1.5	この状況報告にリンクされるよくある脆弱性レポート フレームワーク（CVRF）ファイルをアップデートしました。	諮問ヘッダ	Final	2017-September-19
1.4	更新済修正済みソフトウェア アベイラビリティ情報。	要約および修正済みソフトウェア	Final	2017-May-08
1.3	この アドバイザリに記載される 脆弱性のための エクスプロイトの公共アベイラビリティについての追加された情報。	不正利用事例と公式発表	Final	2017-April-13
1.2	追加された楕円形定義。 状況報告の内容は変更しませんでした。	諮問ヘッダ	Final	2017-April-03
1.1	VTY アクセス リストに追加された情報。	回避策	Final	2017-March-29
1.0	初回公開リリース		Final	2017-March-17

利用規約