Cisco Evolved Programmable Network Manager 7.0.1 リリースノート

初版：2023 年 4 月 26 日

最終更新：2023 年 4 月 26 日

はじめに

本書には、Cisco Evolved Programmable Network Manager 7.0.1 に関する次の情報が記載されています。

追加された機能

ここでは、Cisco EPN Manager 7.0.1 で提供される新機能の一覧を示します。

デバイス サポート

- Cisco A9K-RSP5-X-TR および Cisco A9K-RSP5-X-SE ルートスイッチプロセッサのシャーシビューのサポート
- Cisco A99-RP3-X-TR および Cisco A99-RP3-X-SE ルートプロセッサのシャーシビューのサポート
- Cisco NCS 560-4 RSP4 および Cisco NCS 560-4 RSP4E ルータのシャーシビューのサポート
- IOS-XR 7.8.1 での Cisco NC57-MPA-1FH1D-S のシャーシビューのサポート
- IOS-XE 16.6.4 での Cisco ASR1002-HX ルータのサポート

- Cisco 8000 シリーズ ルータ上の IOS-XR 7.5.1 を搭載した Cisco 88-LC0-34H14FH および Cisco 88-LC0-34H14FH-O ラインカードのシャーシビューのサポート
- Cisco 88-LC0-34H14FH-O ラインカードでの ZR プラガブルのサポート
- IOS-XE 17.9.1 での Cisco N520-X-4G4Z-A および Cisco N520-X-4G4Z-D ルータのサポート
- IOS-XR 7.9.1 での Cisco A9K-20HG-FLEX ラインカードの Cisco DP04QSDD-HE0（QDD-400G-ZRP）プラガブルのサポート
- IOS-XR 7.9.1 上の Cisco NC57-MPA-2D4H-S ラインカードを搭載した Cisco NCS-57C3-MOD-SYS および Cisco NCS-57C3-MODS-SYS シャーシの Cisco DP04QSDD-HE0（QDD-400G-ZRP）プラガブルのサポート
- Cisco NCS 4200 シリーズ デバイスでの IOS-XE 17.9.2a の検証
- Cisco ASR 900 シリーズ ルータでの IOS-XE 17.9.2a の検証
- Cisco ASR 920 シリーズ ルータでの IOS-XE 17.9.2a の検証
- IOS-XE 17.9.2a を搭載した Cisco Catalyst 8000V の基本的なサポート

ライセンシング

- Cisco Crosswork Network Controller および Cisco Crosswork Network Services Orchestrator に応じた Cisco EPN Manager RTM ライセンスの調整

追加されたデバイス/OS のサポート

ここでは、Cisco EPN Manager 7.0.1 で提供される新しいサポートについて説明します。すべてのサポート情報のリストについては、ウェブ GUI の右上にある歯車アイコンをクリックし、[ヘルプ（Help）] > [サポートされるデバイス（Supported Devices）] を選択します。Cisco EPN Manager でサポートされるデバイスの詳細については、サポートされるデバイスツールのページ [英語] を参照してください。

Cisco Network Convergence System 5700 シリーズ ルータ：新しいオペレーティングシステムのサポート

デバイス モデル	デバイスの OS
Cisco NCS 5700 ルータ	IOS-XR 7.8.2
Cisco NCS 5700 ルータ	IOS-XR 7.9.1

Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ：新しいオペレーティングシステムのサポート

デバイス モデル	デバイスの OS
Cisco ASR 9000 ルータ	IOS-XR 7.8.2
Cisco ASR 9000 ルータ	IOS-XR 7.9.1

Cisco Network Convergence System 540 シリーズ ルータ：新しいオペレーティングシステムのサポート

デバイス モデル	デバイスの OS
Cisco NCS 540 ルータ	IOS-XR 7.8.2
Cisco NCS 540 ルータ	IOS-XR 7.9.1

Cisco 8000 シリーズ ルータ：新しいオペレーティングシステムのサポート

デバイス モデル	デバイスの OS
Cisco 8000 ルータ	IOS-XR 7.8.2
Cisco 8000 ルータ	IOS-XR 7.9.1

Cisco Network Convergence System 5500 シリーズ：新しいオペレーティングシステムのサポート

デバイス モデル	デバイスの OS
Cisco NCS 5500 シリーズ	IOS-XR 7.8.2
Cisco NCS 5500 シリーズ	IOS-XR 7.9.1

Cisco Network Convergence System 560 シリーズ ルータ：新しいオペレーティングシステムのサポート

デバイス モデル	デバイスの OS
Cisco NCS 560 ルータ	IOS-XR 7.8.2
Cisco NCS 560 ルータ	IOS-XR 7.9.1

Cisco Network Convergence System 1000 シリーズ：新しいオペレーティングシステムのサポート

デバイス モデル	デバイスの OS
Cisco NCS 1010 ルータ	IOS-XR 7.9.1

サポートされているインストール/アップグレードパス

次の表に、以前のバージョンから Cisco EPN Manager 7.0.1 へのインストール/アップグレードに有効なパスを示します。

現在の Cisco EPN Manager バージョン	Cisco EPN Manager 7.0.1 へのインストールパス
Cisco EPN Manager 7.0.0	Cisco EPN Manager 7.0.0 > 7.0.1

Cisco EPN Manager バージョンのインストールの前提条件と手順については、関連するインストール ガイドを参照してください。

非 HA 展開の更新のダウンロードとインストール

このセクションでは、Cisco EPN Manager 7.0.1 をダウンロードして、非 HA 展開用の既存の Cisco EPN Manager 7.0 がインストールされている環境にインストールする方法について説明します。

手順

ステップ 1 左側のサイドバーで、[管理（Administration）] > [ライセンスとソフトウェアアップデート（Licenses and Software Update）] > [ソフトウェアアップデート（Software Update）] を選択します。

ステップ 2 EPNM GUI から [Cisco.comからのダウンロード（Download from Cisco.com）] オプションを使用するか、ブラウザから Cisco.com に直接ログインして、最新のアップデートをダウンロードします。ファイルには、プレフィックス **cepnm7.0-ppX- buildxxx.ubf** が付きます。

ステップ 3 ファイルが保存された場所に応じて、[ローカルコンピュータからアップロード（Upload from local computer）] または [サーバーのローカルディスクからコピー（Copy from server's local disk）] を選択します。

ステップ 4 ファイルがロードされたら、EPN Manager アップデートに関連付けられている [インストール（Install）] ボタンをクリックします。インストールが完了すると、サーバーが再起動します。

ステップ 5 インストールを続行するには、確認メッセージのダイアログボックスで [はい（Yes）] をクリックします。

（注） インストールが完了すると、サーバーが再起動します。

ステップ 6 既存のファイルを上書きするかどうかを確認するメッセージが表示された場合は、[はい（Yes）] をクリックします。

インストールが成功すると、ステータスが [インストール済み（Installed）] に変わります。Cisco EPN Manager が自動再起動し、しばらくの間 GUI にアクセスできません（最大 1 時間かかる場合があります）。

ステップ 7 Cisco EPN Manager サービスのステータスを確認します。

a) Cisco EPN Manager サーバーとの SSH セッションを開始し、Cisco EPN Manager CLI 管理者ユーザーとしてログインします。

b) **ncs status** コマンドを実行して、ヘルスモニター、データベース、NMS、SAM デーモン、DA デーモン、コンプライアンスエンジンのサービスが稼働していることを確認します。最適な Cisco EPN Manager 機能を使用するには、すべてのサービスが稼働している必要があります。

ステップ 8 Cisco EPN Manager GUI にアクセスできる場合は、ログインして、[ソフトウェアアップデート（Software Update）] ページでパッチのステータスが [インストール済み（Installed）] になっていることを確認します。

すべてのデバイスのインベントリとデータベースの同期（既存の展開のみ）

以前のバージョンの Cisco EPN Manager を使用している場合（つまり、新規インストールではない場合）、デバイスで同期操作を実行します。同期操作では、物理インベントリと論理インベントリの情報を収集し、その情報をデータベースに保存するように Cisco EPN Manager に指示します。

手順

ステップ 1 [モニター（Monitor）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 すべてのデバイスを選択し、[同期（Sync）] をクリックします。

HA 展開の更新のダウンロードとインストール

外部の認証および承認を使用している場合は、インストール後に、最新のアップデートを取得するために、ユーザー タスク情報を AAA サーバーにエクスポートする必要があります。

（注） プライマリおよびセカンダリ HA サーバーへのパッチ適用中、両方のサーバーがダウン状態になります。

手順

はじめる前に

ステップ 1 HA を有効にしたときに作成したパスワード（認証キー）があることを確認します。セカンダリ サーバーにパッチをインストールするときに必要です。

ステップ 2 データをバックアップします（データをバックアップする手順については、『Cisco Evolved Programmable Network Manager 7.0 User and Administrator Guide』[英語] を参照してください）。

サーバーのセッションタイムアウトを増やす

次の手順に従って、プライマリサーバーとセカンダリサーバーのタイムアウトを 30 分から 90 分に増やします。

手順

ステップ 1 Linux CLI ルート ユーザーとしてログインします。

ステップ 2 次のコマンド（1 行）を実行して、**/opt/CSCOlumos/tomcatSWUpdate/webapps/ROOT/WEB-INF/** にある web.xml ファイルのバックアップを保存します。

```
cp /opt/CSCOlumos/tomcatSWUpdate/webapps/ROOT/WEB-INF/web.xml
/opt/CSCOlumos/tomcatSWUpdate/webapps/ROOT/WEB-INF/web.xml.orig
```

ステップ 3 web.xml ファイル（**/opt/CSCOlumos/tomcatSWUpdate/webapps/ROOT/WEBINF/web.xml**）で、次を検索します。

<session-timeout>30</session-timeout>

ステップ 4 セッション タイムアウトを 90 分に変更します。

```
<session-timeout>90</session-timeout>
```

ステップ 5 Cisco EPN Manager CLI 管理者ユーザーとして、手動でサーバーを停止し、再起動します。

```
ncs start
ncs stop
```

ステップ 6 次のコマンドを使用して、すべてのサービスが起動していて実行されていることを確認します。

```
ncs status
```

HA 設定の削除

手順

ステップ 1 Cisco EPN Manager GUI に管理者権限を持つユーザーとしてログインします。

ステップ 2 左側のサイドバーで、[管理（Administration）] > [設定（Settings）] > [高可用性（High Availability）] の順に選択します。

ステップ 3 [HA設定（HA Configuration）] ページで [削除（Remove）] をクリックします。

ステップ 4 プライマリサーバーで、[管理（Administration）] > [設定（Settings）] > [高可用性（High Availability）] に移動し、[コンフィギュレーションモード（Configuration Mode）] フィールドに「HA未設定（HA Not Configured）」と表示されていることを確認します。

ステップ 5 セカンダリサーバーページのヘルスモニターページにログインし、[状態（State）] タブに「HA未設定（HA Not Configured）」と表示されていることを確認します。

プライマリサーバーとセカンダリサーバーへのデバイスパックとポイントパッチのインストール

手順

ステップ 1 開始する前に、HA を有効にしたときに作成したパスワード（認証キー）があることを確認します。セカンダリサーバーにメンテナンスパックをインストールする必要があります。

ステップ 2 進行中のバックアップがないことを確認します。

ステップ 3 セカンダリサーバーで、ソフトリンクを使用してタイムゾーンを更新します。

```
ln -sf /usr/share/zoneinfo/$(grep ^clock /storedconfig/active/startupconfig
| cut -d " " -f 3) /etc/localtime
```

これにより、フェールオーバー後にコンプライアンス サーバーがセカンダリ サーバー上で起動して稼働するようになります。

プライマリサーバーへのデバイスパックとポイントパッチのインストール

手順

ステップ 1 左側のサイドバーから、[管理（Administration）] > [ライセンスとソフトウェアアップデート（Licenses and Software Update）] > [ソフトウェアアップデート（Software Update）] を選択します。

ステップ 2 EPNM GUI から [Cisco.comからのダウンロード（Download from Cisco.com）] オプションを使用するか、ブラウザから Cisco.com に直接ログインして、最新のアップデートをダウンロードします。ファイルには、プレフィックス **cepnm7.0-ppx- buildxxx.ubf** が付きます。

ステップ 3 ファイルが保存された場所に応じて、[ローカルコンピュータからアップロード（Upload from local computer）] または [サーバーのローカルディスクからコピー（Copy from server's local disk）] を選択します。

ステップ 4 ファイルがロードされたら、EPN Manager アップデートに関連付けられている [インストール（Install）] ボタンをクリックします。

ステップ 5 インストールを続行するには、確認メッセージのポップアップ ウィンドウで [はい（Yes）] をクリックします。

ステップ 6 Cisco EPN Manager が自動的に再起動し、Cisco EPN Manager の Web GUI にしばらくアクセスできなくなります。（最大 1 時間かかる場合があります）

ステップ 7 「ハードウェアと NTP クロックの同期」で説明されているように、プライマリサーバーとセカンダリサーバーの両方でハードウェアクロックと NTP クロックを同期し、各サーバーのクロックが相互に同期されていることを確認します。

（注） デバイスパックおよびポイントパッチをインストールすると Cisco EPN Manager が再起動されるため、同期クロック操作でのサービスの再起動は無視できます。

セカンダリサーバーへの Cisco EPN Manager のインストール

手順

ステップ 1 セカンダリサーバーの Web ページにログインします。

ステップ 2 認証キーを入力して、[ログイン（Login）] をクリックします。

ステップ 3 [ソフトウェアアップデート（Software Update）] ボタンをクリックします。

ステップ 4 ログインページが表示されます。Cisco EPN Manager に管理者としてログインします。

ステップ 5 Cisco EPN Manager GUI で [Cisco.com] オプションから [ダウンロード（Download）] オプションを使用するか、ブラウザから Cisco.com に直接ログインして、最新のアップデートをダウンロードします。ファイルには、プレフィックス **cepnm7.0-ppx- buildxxx.ubf** が付きます。

ステップ 6 ファイルが保存された場所に応じて、[ローカルコンピュータからアップロード（Upload from local computer）] または [サーバーのローカルディスクからコピー（Copy from server's local disk）] を選択します。

ステップ 7 ファイルがロードされたら、EPN Manager アップデートに関連付けられている [インストール（Install）] ボタンをクリックします。

ステップ 8 インストールを続行するには、確認メッセージのポップアップ ウィンドウで [はい（Yes）] をクリックします。

Cisco EPN Manager が自動的に再起動し、Cisco EPN Manager の Web GUI にしばらくアクセスできなくなります。（最大 1 時間かかる場合があります）

セカンダリサーバーでのインストールの検証

手順

ステップ 1 Cisco EPN Manager サーバーとの SSH セッションを開始し、Cisco EPN Manager CLI 管理者ユーザーとしてログインします。

ステップ 2 **ncs status** コマンドを実行して、少なくともヘルスモニター、データベース、NMS、SAM デーモン、DA デーモン、コンプライアンスエンジンのサービスが稼働していることを確認します。

最適な Cisco EPN Manager 機能を使用するには、すべてのサービスが稼働している必要があることに注意してください。

ステップ 3 Web GUI にアクセスできたら、セカンダリ サーバーの [HM Web] ページでインストールとバージョンを確認します。

ここで、serverIP はセカンダリ サーバーの IP アドレスまたはホスト名です。

ステップ 4 認証キーを入力して、[ログイン（Login）] をクリックします。

ステップ 5 [アップロード済みのアップデートファイル（Uploaded Update Files）] タブで、MPx ubf ファイル（cepnm.7.0-ppx- buildxxx.ubf の形式）が表示されており、[使用中（In Use）] ステータスが [はい（Yes）] になっていることを確認します。

ステップ 6 次のコマンドを実行して、すべてのサービスが起動していて実行されていることを確認します。

```
ncs status
```

HA の有効化と HA ステータスの確認

手順

ステップ 1 高可用性を有効にします。

a) Cisco EPN Manager Web GUI に管理者権限を持つユーザーとしてログインします。
b) 左側のサイドバーメニューで、[管理（Administration）] > [設定（Settings）] > [高可用性（High Availability）] の順に選択します。
c) [HA設定（HA Configuration）] をクリックしてから、セカンダリサーバーの IP アドレス、セカンダリサーバーの認証キー、および Cisco EPN Manager が HA の状態変更通知を送信する電子メールアドレスを入力します。
d) HA セットアップで仮想 IP アドレッシングを使用している場合（プライマリサーバーとセカンダリサーバーが同じサブネットにある場合）は、[仮想IPの有効化（Enable Virtual IP）] チェックボックスをオンにして、1 つ以上の仮想 IP アドレスを入力します。
e) [保存（Save）] をクリックして、サーバーが同期されるまで待ちます。
f) 設定モードが [HA 対応（HA Enabled）] になっていることを確認します。

ステップ 2 プライマリ サーバーの HA ステータスを確認します。

a) 左側の [HA ステータス（HA Status）] をクリックします。
b) [現在のステータス モード（Current State Mode）] に [プライマリ アクティブ（Primary Active）] と表示されていることを確認します。

ステップ 3 セカンダリサーバーの HA ステータスを確認します。

a) セカンダリサーバーの Web ページにログインします。
b) 認証キーを入力して、[ログイン（Login）] をクリックします。

c) [現在のステータスモード（Current State Mode）] が [セカンダリ同期中（Secondary Syncing）]（緑色のチェックマーク付き）になっていることを確認します。

すべてのデバイスのインベントリとデータベースの同期（既存の展開のみ）

以前のバージョンの Cisco EPN Manager を使用している場合（つまり、新規インストールではない場合）、デバイスで同期操作を実行します。同期操作では、物理インベントリと論理インベントリの情報を収集し、その情報をデータベースに保存するように Cisco EPN Manager に指示します。

手順

ステップ 1 [モニター（Monitor）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 すべてのデバイスを選択し、[同期（Sync）] をクリックします。

特記事項

アップグレードの問題

- FTP と TPTP は、デフォルトで無効になります。
- 温度のアクティブなしきい値超過アラーム（TCA）はアクティブなままになり、自動ではクリアされません。これらのアラームは手動でクリアしてください。
- ISIS リンクを表示するには、デバイスを再同期する必要があります。
- LDP 機能関連の情報を表示するには、LDP 対応デバイスを再同期する必要があります。
- インバウンド/アウトバウンドエラーおよびインバウンド/アウトバウンド廃棄の TCA は、インターフェイス ヘルス モニタリング ポリシーで再作成する必要があります。

キャリアイーサネット回線プロビジョニングに関する制限事項

- 古いプローブ名形式を使用したサービスのプロモーションがサポートされるようになりました。これらのプローブは、プロモーション後に適切な標準 OAM プロファイル名とともにユーザーインターフェイスに表示されます。
- サンプルプロファイル：profile PM2_3_8_CoS5_DM type cfm-delay-measurement
- EPN Manager ではカスタムプロファイル名がサポートされていますが、別の命名形式でブラウンフィールドサービスを変更すると、既存のカスタムプロファイルが削除され、サポートされている命名形式で新しいプロファイルが追加されます。

- インベントリモデルでは、サービスに関連付けられていないプロファイルは正しく表示されません。
- プロファイル数の検証制限は 100 です。100 個の既存のプロファイルの後に新しい SLA 操作プロファイルを作成すると、デバイスでエラーが生成され、展開が失敗します。

HTTPS および TLS のセキュアチャネル通信には TLS 1.2 が必要です。

Transport Layer Security（TLS）1.2 のみが、HTTPS および TLS 関連の安全な通信（RADIUS EAP-TLS など）でサポートされます。

TLS 1.0、TLS 1.1、およびすべてのバージョンの SSL のサポートは、セキュリティの脆弱性のため無効になっています。

これは、HTTPS/TLS を使用して Cisco EPN Manager を使用するすべてのピアシステムとクライアントが、TLS 1.2 をサポートする必要があることを意味します。TLS 1.2 がサポートされない場合は、これらのシステムをアップグレードする必要があります。Cisco EPN Manager のマニュアルでは、可能な限り、影響を受ける可能性のあるシステムを強調しています。必要に応じて、シスコの担当者にお問い合わせの上、この点に関してサポートをご依頼ください。

調整レポートの制限事項

サービスをプロビジョニングするときに、属性の値を指定していない場合、その属性のプロビジョニングされた値は、調整レポートで「欠落（Missing）」と表示されます。デバイスでこの属性のデフォルト値が設定される場合がありますが、Cisco EPN Manager では設定されません。

ME 1200 デバイスの制限事項

Y.1564 パフォーマンステストは、送信元/宛先が ME 1200 デバイスである場合は機能しません。

アラーム通知ポリシーの編集に関する制限事項

既存のカテゴリのアップグレード条件が 5.1 のカテゴリの条件と異なる場合、アップグレード後の条件は一致しません。その結果、一致しないイベントについては、ポリシーが作成されないか、UI の選択が行われない可能性があります。この場合、アップグレードされたポリシーを削除して、新しいポリシーを作成する必要があります。

IOS-XE 16.8.1 を実行している NCS 4200 デバイスの制限事項

次の機能は、IOS-XE 16.8.1 を実行している NCS 4200 デバイスでは機能しません。

- Alarm プロファイル
- GUI からの SONET LOP および CT3 LOP の設定
- SONET/T1/T3 HOP/LOP での管理上の shut/no shut 機能

NCS540 および NCS5500 デバイスの制限事項

NCS540 および NCS5500 デバイス シリーズでは、障害 OAM、ラップ保護、および BFD はサポートされません。

PTP コマンドの設定に CLI テンプレートを使用する

ソフトウェアバージョン 16.9.1 の ASR920 デバイスでは、1588 PTP コマンドを実行するために IEEE 1588-2008 BC/MC ライセンスが必要です。

PTP テンプレートでは設定とインベントリがサポートされていません

PTP テンプレートを使用してプッシュされた設定をモデリングする動作は、期待どおりに機能しない可能性があります。これは、PTP テンプレートを介してプッシュされるすべての設定に対してモデルが確立されていない可能性があるためです。設定/インベントリは、これらの設定ではサポートされていません。

10.00.10、10.01.00、10.03.00 のサポートの廃止

Cisco NCS 2002、2006、および 2015 デバイスでは、ONS 10.00.10、10.01.00、10.03.00 ONS 10.00.10、10.01.00、および 10.03.00 はサポートされなくなりました。

データセンターのデバイスライフサイクルのサポートのみ

Cisco EPN Manager は、UCS コンピューティングシステム、CSR 1000v、および Nexus シリーズデバイスの基本的なライフサイクルサポートを提供しますが、データセンタートポロジは提供しません。

ギガビットポートのサブインターフェイスでの LINK_DOWN アラーム

LINK_DOWN アラームは、ギガビットポートのサブインターフェイスでリンクがダウンしている場合は生成されません。

Cisco EPN Manager のバグ

未解決のバグ

次の表に、Cisco EPN Manager リリース 7.0.1 の未解決のバグを、以下の条件に従って示します。

- 重大度 1、2、および優先度の高い重大度 3 の未解決のバグ
- お客様から報告されたすべての未解決のバグ

- Cisco EPN Manager のワークフローに影響を与える可能性が高い、大きな影響を及ぼすバグ。

[識別子（Identifier）] リンクをクリックすると、バグ検索ツールでバグの影響と回避策が表示されます。このツールを使用して、未解決のバグのステータスを追跡します。

バグ	説明
CSCwe73405	コードミラー 3.19.0 CVE-2020-7760 の脆弱性
CSCwc78979	Bellatrix：コヒーレント DSP が POST 変更操作の応答でエラーを出力する
CSCwd12284	[GA]：デバイスの管理ステータスが変更された場合に、UI でコヒーレントポートが部分的に、またはまったく表示されない
CSCwd99608	[GA]：XML からのスパン損失値がデバイスと一致しない

解決済みのバグ

次の表に、お客様から報告されたバグのうち、Cisco EPN Manager 7.0.1 で解決済みのバグを示します。

解決済みのバグの詳細については、バグ検索ツールを参照してください。

バグ	説明
CSCwe10195	EPNM 7.0GA I151 Build Nessus で脆弱性の高いプラグイン ID 168497 が検出される
CSCwe12754	NCS 1010：アラームマネージャ設定を有効にした後、デバイスの手動同期が必要になる
CSCwe21883	EPNM 6.1.1.1 Build33：Nessus で脆弱性が検出される
CSCwe27958	L3VPN タグなしサービスプロビジョニングの作成時に例外がスローされる
CSCwe37602	EPNM 5.0.2.5 Build769：Nessus で脆弱性が検出される
CSCwe38852	7.0.1 - i153B の署名されていない UBF #28 のインストールに失敗した
CSCwe47917	Apache Tomcat 9.0.0.M1 < 9.0.71
CSCwe62265	l2vpn サービスで y1564 テストを実行した後に 7.0.1 154B > のサーバークラッシュが発生した
CSCwe66098	jackson-databind 2.13.3 の脆弱性
CSCwe66142	netty 4.1.72.Final の脆弱性

バグ	説明
CSCwe73473	commons-beanutils - multiple versions の脆弱性
CSCwe77311	EPNM_7_0_1_GA：フラッシュの消去オプションが有効になっていると、c8000v デバイスのイメージアクティブ化が失敗する
CSCwe83895	EPNM7.0.1GA 155A Build105 Nessus で脆弱性が検出される
CSCwf00112	38 レポートテンプレートが [レポート起動パッド（Report Launch Pad）] にのみ表示される
CSCwe07091	Cisco Evolved Programmable Network Manager のコマンドインジェクション脆弱性
CSCwe14957	7.0 GA BnR アップグレード、一部のレポートのアップグレード中にレポートのフィルタ条件が更新されない
CSCwe17035	EPNM 7.0GA I151C：Nessus で脆弱性が検出される
CSCwe23019	db_size.sh 内のハードコードされた数字 650 が原因で、バックアップジョブが db をバックアップできない
CSCwe23573	EPNM 6.0.2：HMMain でのメモリリーク – CARS JNI 呼び出し
CSCwe24786	NCS2K の自己応答属性に関するループバックの setTP で管理状態および操作状態の値が適用されない
CSCwe29279	インベントリモジュールでの DB 接続リーク
CSCwe29295	NBI-restconf からの DB 接続リーク
CSCwe36146	光レガシー（非 WSON）回線の検出状態が部分的である
CSCwe36292	保護プロファイルが存在しないため、OTN サービスのプロビジョニングが無効エラーにより失敗する
CSCwe42670	NCS1K4-2-QDD-C-K9：マックスポンダ スライス モードで、EPNM を使用してスライスを削除できない
CSCwe43155	SONET を保護された状態から ACR 設定で動作するように変更すると、ループバック インターフェイスが削除される
CSCwe47418	NCS 5001 プラットフォームで clock コマンドが失敗する

バグ	説明
CSCwe47889	GA > 7.0.1 > MLT が SR の access-evpl に対してエラーをスローする
CSCwe48459	3*100 または 4*100 が作成された場合、EPNM がブレークアウトを hwmodule にプッシュしない
CSCwe48959	notset を実行すると、dac rate でデフォルト値が表示されない
CSCwe48980	設定済み TX Power/CD-MIN/CD-MAX の境界値が 7.9.1 で変更される
CSCwe51877	NCS2K の波長の setTP で、自己応答で「tp.wavelength」により波長ではなく周波数が取得される
CSCwe54471	7.0/7.1：CEM 変更により検出が部分的になる：TdmCmPWCnPrtclEndpnt オブジェクトが検出されない
CSCwe56282	Flex アルゴリズムがセグメントルーティングにおける MBC での保存に失敗する
CSCwe57774	IOS XR 6.9.1 以降で動作しないインターフェイスの非動的サポートを表示する
CSCwe61615	REPT EVT FXFR イベントにより、nms-optical-fault ログに例外が表示され、GUI にイベントが表示されない
CSCwe62723	EPNM_7_0_1_GA：c8000v イメージのアクティブ化中に、boot config エラーメッセージの更新失敗が観察された
CSCwe66205	Bright ZRP：ASR9912：[コントローラ（Controllers）] --> [Optics0/3/0/0] --> [DAC レート（DAC Rate）] フィールドを編集できない
CSCwe66810	7.0.1 RON SOL > EPNM が、デバイスで OTS ポートを管理上ダウン/アップにした後も、管理ダウンとして表示し続ける
CSCwe67273	wss4j 1.6.9 の脆弱性
CSCwe67276	Bright ZRP：コヒーレントポートで同じ SD および SF BER 値が選択されている場合、EPNM はエラー表示をスローしない
CSCwe67383	Bright ZRP：EPNM で設定された Tx 電力範囲は、-150 ～ 0 ではなく、-150 ～ 50 にする必要がある

バグ	説明
CSCwe67571	postgresql-jdbc 9.4.1212.jre7 の脆弱性
CSCwe68524	mina 2.0.5、2.0.1 の脆弱性
CSCwe68710	tzinfo 1.2.2 の脆弱性
CSCwe68909	cisco-resource-physical：管理対象外のデバイスがある場合、深度 ATT のノードが機能しない
CSCwe70051	Bright ZRP：ASR9K：[コントローラ（Controllers）] --> [光（Optics）]：デバイスに表示されているすべての DAC レートが EPNM でサポートされている必要がある
CSCwe72263	Bright ZRP：ASR9k：[1528773] を設定した後、[設定波長（Configured Wavelength）] が正しく更新されない
CSCwe73143	回線へのループバック参照がデバイスに合わせて更新されない
CSCwe73797	i18n - deviceTrend - デバイス正常性ダッシュボードが見つからない
CSCwe73888	7.7.1 に関して、NCS1010 OLC スパン損失のデータが 7.9.1 から欠落している
CSCwe73958	OSPF リンクのダウンは、NCS1010 の EPNM における物理リンクのダウンを生じさせない
CSCwe76131	範囲検証で、設定された Tx 電力/CD-Min/CD-MAX に引き続き古い値が表示される
CSCwe76315	OCHCC Prov ウィザードで、使用可能なすべてのクライアントポートが一覧表示されない
CSCwe81224	ブレークアウト情報がデバイスで作成されていると、EPNM で更新されない
CSCwe81345	NCS1K4：カードから光学部品を物理的に取り外した後、インベントリステータスが更新されない
CSCwe81394	DAC レート、デバイスが受け入れる、EPNM が受け入れない、受け入れないというエラーメッセージが明確ではない
CSCwe83247	Bright ZRP：エラーメッセージに、設定された Tx 電力の古い値の範囲が引き続き表示される

バグ	説明
CSCwe91017	[管理（Administration）] -> [システム設定（System Settings）] の [アラームとイベント（Alarms and Events）] が空になる
CSCwc64497	6.1 インストールガイドの更新
CSCwd19417	MPLS-LDP では、[ダウンストリーム最大ラベル（Downstream Max Label）] には 32768 までの値のみを設定できるが、デバイスには 1048575 まで設定できる
CSCwd62509	[アラームポリシー（Alarm Policies）] ページの XSS 脆弱性
CSCwe00397	週間スケジュールレポートの [毎（Every）] フィールドには、GA と LA の両方に最大値に関する問題がある
CSCwe19705	CE 更新のシナリオが EVPN サービスで失敗する：7.0GA | 151C BUILD#595
CSCwe36308	restconf を使用して回路を作成しているときに、[ラベル（Label）] パラメータが指定されていないと、回路の作成に失敗する
CSCwe46388	無効な距離での OTDR スキャンでは、「400 Bad Request」が表示される必要があるが、エラー「 500」が表示される
CSCwe56299	MPLS-LDP では、[ダウンストリーム最大ラベル（Downstream Max Label）] には 32768 までの値のみを設定できるが、デバイスには 40960 まで設定できる
CSCwe62189	setTP 光ファイバ属性の検証で、エラーコードは「400 Bad Request」である必要があるが、エラー「500」が表示される
CSCwe62196	setTP NNI コントローラの検証で、「400 Bad Request」ではなく「500」が表示され、エラータグも変更された
CSCwe62972	EPN - インストール - 証明書の設定が初期化されない
CSCwe69943	デバイスでは CD-MIN/CD-MAX を 0 に設定できるが、EPNM が警告をスローする
CSCwd90369	GA：ローカリゼーション：光物理/イーサネット PM ダッシュボードで、PM カウンタのタイトルがローカライズされていない

バグ	説明
CSCwe36277	センサーグラフ：ツールチップの値が四捨五入され、小数点以下 3 桁の数に切り上げられる
CSCwe48356	ユーザーがインライン編集を開いてキャンセルボタンを選択すると、トーストメッセージが表示される
CSCwe82966	エラーメッセージにフィールド名が完全に表示されない
CSCwe78745	コンポーネント glibc の重大な CVE。最新バージョンにアップグレードする
CSCwe78840	コンポーネント openssl の重大な CVE。最新バージョンにアップグレードする
CSCwe15015	7.0-GA および LA：L3VPN LSP OAM が失敗する
CSCwe17532	300G トランクを使用した LMP 設定が失敗し、エラーメッセージが表示される
CSCwe31942	NCS1004：I360 の [光物理（OpticalPhysical）] タブにトランク光ファイバポートの [Tx電力（TxPower）] および [Rx電力（RxPower）] がない
CSCwe32001	[レポート（Report）] > [レポート起動パッド（Report Launchpad）] > [任意のカードを選択（Select Any card）]
CSCwe67260	jettison 1.2 - design-tool-blueprint-webapp の脆弱性
CSCwe75027	アクションプロファイルをインポートしても、すべてのデータがインポートされない（たとえばキューイング アクション データがインポートされない）
CSCwe83417	EPN - 障害 - NCS 4216 アラーム再同期機能がファンアラームで失敗する

Cisco EPN Manager のバグに関する情報を取得する

Cisco EPN Manager のバグに関する最新情報を取得するには、バグ検索ツール（BST）を使用します。BST を使用すると、パートナーとお客様は製品、リリース、キーワードに基づいてソフトウェアバグを検索し、バグ詳細、製品、バージョンなどの主要データを集約することができます。

Cisco EPN Manager のバグは、デバイスのプラットフォームまたはオペレーティングシステムの不具合が原因で発生する可能性があります。このような場合、ハードウェア/オペレーティングシステムのバグが解決されると、Cisco EPN Manager のバグが解決されます。

手順

ステップ 1 バグ検索ツールにログインします。

a) https://tools.cisco.com/bugsearch/ に移動します。

b) [ログイン（Log In）] 画面で、登録済みの Cisco.com ユーザ名およびパスワードを入力し、[ログイン（Log In）] をクリックします。

（注） Cisco.com のユーザー名とパスワードを持っていない場合、http://tools.cisco.com/RPF/register/register.do で登録できます。

ステップ 2 このバージョンのすべてのバグを一覧表示するには、[製品（Product）] フィールドの横にある [リストから選択（Select from list）] ハイパーリンクをクリックし、製品を選択します。

a) [クラウドおよびシステム管理（Cloud And Systems management）]>[ルーティングおよびスイッチング管理（Routing and Switching Management）]>[Cisco Evolved Programmable Network (EPN) Manager] の順に選択し、必要な製品バージョンを選択します。

b) 結果が表示されたら、フィルタツールとソートツールを使用して、ステータス、重大度、最近の変更、サポートケースが関連付けられているかどうかなどに従って、バグを検索します。

バグ ID またはキーワードを使用してバグを検索することができます。詳細については、バグ検索ページの右上にある [ヘルプ（Help）] をクリックしてください。

関連資料

Cisco EPN Manager 7.0.1 で使用可能なすべてのドキュメントの一覧については、『Cisco Evolved Programmable Network Manager 7.0』[英語] を参照してください。

アクセシビリティ機能

Cisco EPN Manager 7.0.1 のアクセシビリティ機能のリストについては、accessibility@cisco.com にお問い合わせください。

すべての製品ドキュメントにアクセスできます。音声、点字、または大きな文字の製品マニュアルが必要な場合は、accessibility@cisco.com にお問い合わせください。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービスリクエストの送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

Cisco 製品資料の更新情報には、シスコの新規および改訂版の技術マニュアルがすべて表示されます。この RSS フィードを登録するか、リーダーアプリケーションを使用してコンテンツを直接デスクトップに配信することもできます。RSS フィードは無料のサービスです。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。