Cisco Unified Communications Manager Express な脆弱性

High

アドバイザリーID : cisco-sa-20090923-cme

初公開日 : 2009-09-23 16:00

バージョン 1.1 : Final

CVSSスコア : 7.6

回避策 : No Workarounds available

Cisco バグ ID : CSCsq58779

CVE-2009-2865

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 Unified Communications Manager Express （CME）およびエクステンションモビリティ 機能のために設定される Cisco IOS® デバイスはバッファオーバーフローの脆弱性に脆弱である。この脆弱性の不正利用の成功は任意 の コードの実行か影響を受けたデバイスのサービス拒否（DoS）条件という結果に終るかもしれません。

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。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-cme で掲示されます。

注: 2009 年 9 月 23 日の IOS アドバイザリ バンドル公開には 11 件の Security Advisory が含まれています。 10 件のアドバイザリは Cisco IOS ソフトウェアの脆弱性に対処するもので、 1 件は Cisco Unified Communications Manager の脆弱性に対処するものです。 各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決するリリースを記載しています。

"Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" の個々の公開リンクは次のリンク内に掲載されています:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

該当製品

Cisco IOSデバイスは、Cisco Unified CME および エクステンションモビリティ 機能のために設定される Cisco Unified Communications 500 シリーズを含んで、影響を受けています。

脆弱性のある製品

Cisco Unified CME およびエクステンションモビリティのために設定される Cisco IOSデバイスは **show running-config コマンドが**発行されるとき次の出力が含まれています:

```
ephone [Ethernet phone tag]
  ...
  logout-profile [logout-profile tag]
```

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 イメージ名は「バージョン」および Cisco IOS ソフトウェアリリース名によって、続かれて括弧内に表示する。 他のシスコ デバイスでは、**show version** コマンドが存在しなかったり、別の出力が表示されたりします。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
    Router#show version
    Cisco Internetwork Operating System Software
    IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
    Technical Support: http://www.cisco.com/techsupport
    Copyright (c) 1986-2008 by cisco Systems, Inc.
    Compiled Mon 17-Mar-08 14:39 by dchih

    <output truncated>
```

次の例は C1841-ADVENTERPRISEK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 12.4(20)T を実行している Cisco製品を指定したものです:

```
    Router#show version
    Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
    Technical Support: http://www.cisco.com/techsupport
    Copyright (c) 1986-2008 by Cisco Systems, Inc.
    Compiled Thu 10-Jul-08 20:25 by prod_rel_team

    <output truncated>
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide" で確認できます: http://www.cisco.com/warp/public/620/1.html。

脆弱性を含んでいないことが確認された製品

Survivable Remote Site Telephony （ SRST ） モードのために設定される Cisco IOSデバイスは影響を受けていません。

Cisco IOS XR は該当しません。

Cisco IOS XE は影響を受けていません。

Cisco Unified Communications Manager は影響を受けていません。

Cisco Unified CME はエクステンションモビリティ 機能を使用するために設定されて影響を受けていません。

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。

詳細

Cisco Unified CME は Cisco IOS に統合されている拡張 IP テレフォニー ソリューションのコール処理 コンポーネントです。

Cisco Unified CME のエクステンションモビリティ 機能はエンドユーザ用に電話モビリティの利点を提供します。 一時的に物理的 な電話に自身の電話以外アクセスし、個人的な設定を、自身の卓上電話機に割り当てられるディレクトリ番号、speed-dial リストおよびサービスのような利用するユーザ ログイン サービス割り当て電話ユーザ。 電話ユーザは同じパーソナルディレクトリ数を使用してその電話で卓上電話機が自分自身であると呼び出しを作り、受信できます。 エクステンションモビリティ 機能の次の URL を参照して下さい:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmemobl.html

エクステンションモビリティ 機能のログオン セクションの脆弱性は非認証攻撃者が任意 の コードを実行するか、またはサービス拒否（DoS）状態を引き起こすことを可能にするかもしれません。 そのようなパケットは HTTP 要求の形に登録済みの電話 IP アドレスからしか来ることができません。 自動登録機能が有効に なる場合、攻撃者は IP アドレスを登録し、この脆弱性を不正利用するために続いて巧妙に細工された ペイロードを送信できます。 自動登録機能はデフォルトで有効に なります。 自動登録に関する詳細は次のリンクで見つけることができます:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_a1ht.html#wp1031242。

この脆弱性 Cisco バグ ID **CSCsq58779**（登録ユーザのみ）によって当たり、よくある脆弱性および公開（CVE）ID CVE-2009-2865 は割り当てられました。

回避策

エクステンションモビリティをディセーブルにすること以外この脆弱性を、軽減する回避策がありません。 ただし不正利用をさらに困難にするために、自動登録はディセーブルにすることができます。 自動登録は次のコマンドによってディセーブルにすることができます:

```
telephony-service
  no auto-reg-ephone
```

自動登録をディセーブルにする前に、すべての電話 MAC アドレスは明示的に Cisco Unified CME で定義される必要があります。 さもなければ電話は登録されられません。 自動登録に関する詳細は次のリンクで見つけることができます:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_a1ht.html#wp1031242

ネットワークの on Cisco 配置されたデバイスの場合もある追加軽減は次のリンクで利用可能のこのアドバイザリに Cisco によって加えられる軽減情報ドキュメントガイドで利用できます、: http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090923-cme

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、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

いずれの場合も、アップグレードする機器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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。 情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、Cisco IOS のリリース トレインが記載されています。 特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（および、それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。 「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。 特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。 表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャー リリース	修理されたリリースの Â Â Â Â Â 可用性	
Affected 12.0-Based Releases	First Fixed Release（修正された最初のリリース）	**推奨リリース**
該当する 12.0 基づいたリリースがありません。		
Affected 12.1-Based	First Fixed Release（修正された最初のリリース）	**推奨リリース**

Releases		
該当する 12.1 基づいたリリースがありません。		
Affected 12.2-Based Releases	First Fixed Release (修正された最初のリリース)	**推奨リリース**
該当する 12.2 基づいたリリースがありません。		
Affected 12.3-Based Releases	First Fixed Release (修正された最初のリリース)	**推奨リリース**
該当する 12.3 基づいたリリースがありません。		
Affected 12.4-Based Releases	First Fixed Release (修正された最初のリリース)	**推奨リリース**
12.4	脆弱性なし	
12.4GC	脆弱性なし	
12.4JA	脆弱性なし	
12.4JDA	脆弱性なし	
12.4JDC	脆弱性なし	
12.4JDD	脆弱性なし	
12.4JK	脆弱性なし	
12.4JL	脆弱性なし	
12.4JMA	脆弱性なし	
12.4JMB	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MDA	脆弱性なし	
12.4MR	脆弱性なし	
12.4SW	脆弱性なし	
12.4T	脆弱性なし	
12.4XA	脆弱性なし	
12.4XB	脆弱性なし	
12.4XC	脆弱性なし	
12.4XD	脆弱性なし	
12.4XE	脆弱性なし	
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	
12.4XJ	脆弱性なし	
12.4XK	脆弱性なし	
12.4XL	脆弱性なし	
12.4XM	脆弱性なし	
12.4XN	脆弱性なし	

12.4XP	脆弱性なし	
12.4XQ	脆弱性なし	
12.4XR	脆弱性なし	
12.4XT	脆弱性なし	
12.4XV	脆弱性なし	
12.4XW	12.4(11)XW8	12.4(20)T4 12.4(22)T3 12.4(24)T2 ; 23-OCT-2009 で利用可能
12.4XY	12.4(15)XY4	12.4(20)T4 12.4(22)T3 12.4(24)T2 ; 23-OCT-2009 で利用可能
12.4XZ	12.4(15)XZ1	12.4(20)T4 12.4(22)T3 12.4(24)T2 ; 23-OCT-2009 で利用可能
12.4YA	12.4(20)YA1	12.4(20)T4 12.4(22)T3 12.4(24)T2 ; 23-OCT-2009 で利用可能
12.4YB	脆弱性なし	
12.4YD	脆弱性なし	
12.4YE	脆弱性なし	

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の公示か不正利用に気づいていません。

この脆弱性はシスコ内部で発見されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-cme

改訂履歴

リビジョン	2009-September-23	初版リリース

1.0		

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。