Cisco Security Advisory: Cisco Unified Service Monitor and Cisco Unified Operations Manager Remote Code Execution Vulnerabilities

Advisory ID: cisco-sa-20110914-cusm

http://www.cisco.com/warp/public/707/cisco-sa-20110914-cusm.shtml

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。

Revision 1.1

Last Updated 2011 September 22 0617 UTC (GMT)

For Public Release 2011 September 14 1600 UTC (GMT)

目次

要約

Cisco Unified Service Monitor および Cisco Unified Operations Manager ソフトウェアには 2 つの脆弱性が存在します。これらによって、リモートの認証されていない攻撃者が該当サーバで任意のコードを実行できる場合があります。

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。

この脆弱性を軽減する回避策があります。

このアドバイザリは次のリンクに掲載されます。 http://www.cisco.com/warp/public/707/cisco-sa-20110914-cusm.shtml

注： CiscoWorks LAN Management Solution もこれらの脆弱性の影響を受けます。CiscoWorks LAN Management Solution についてのアドバイザリは次のリンクに掲載されています。 http://www.cisco.com/warp/public/707/cisco-sa-20110914-lms.shtml

該当製品

脆弱性が存在する製品

Cisco Unified Service Monitor および Cisco Unified Operations Manager の 8.6 より前の全バージョンが影響を受けます。

Cisco Unified Service Monitor および Cisco Unified Operations Manager ソフトウェアのバージョンを確認するには、**[Administration] > [Software Center (Common Services)] > [Software Update]** に進みます。 [Software Update] ページにライセンスとソフトウェアのバージョンが表示されます。

脆弱性が存在しない製品

CiscoWorks LAN Management Solution を除く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 Service Monitor および Cisco Unified Operations Manager は、Cisco Unified Communications Management Suite に含まれる製品であり、Cisco Unified Communications System がサポートするアクティブ コールを継続的に監視する手段を提供します。

Cisco Unified Service Monitor および Cisco Unified Operations Manager ソフトウェアには 2 つの脆弱性が存在します。これらによって、リモートの認証されていない攻撃者が該当サーバで任意のコードを実行できる場合があります。これらの脆弱性は、該当するサーバに TCP ポート 9002 を介して一連の巧妙に細工されたパケットが送信されることによって引き起こされます。

これらの脆弱性いずれも Cisco Bug ID CSCtn42961 （ 登録ユーザのみ ）として文書化され、CVE ID CVE-2011-2738 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、個々のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次の URL にて CVSS に関する FAQ を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを以下の URL にて提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x

CSCtn42961 - isco Unified Service Monitor Remote Code Execution Vulnerabilities **Calculate the environmental score of**					
CVSS Base Score - **10**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **8.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

これらの脆弱性が悪用されると、リモートの認証されていない攻撃者が該当サーバで任意のコードを実行できる場合があります。

ソフトウェア バージョンおよび修正

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/ および本アドバイザリ以降に公開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。情報が不明確な場合は、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。

これらの脆弱性は Cisco Unified Service Monitor および Cisco Unified Operations Manager ソフトウェア バージョン 8.6 で修正されています。

Cisco Unified Service Monitor および Cisco Unified Operations Manager ソフトウェアは次のリンク先からダウンロードできます。

http://www.cisco.com/cisco/software/navigator.html?mdfid=280110371&i=rm

回避策

アプリケーションが同一システム上で DFM ブローカーとして稼動している Cisco Unified Service Monitor または Cisco Unified Operations Manager では、管理者は回避策として以下のレジストリキーの変更を行うことができます。

レジストリ キー **HKEY_LOCAL_MACHINE¥SOFTWARE¥Cisco¥Resource Manager¥CurrentVersion¥Daemons¥DfmBroker** の **Args** パラメータを **--output --port=9002** から **--output --port=9002 --accept=127.0.0.1,<hostname>** に変更します。

注： <hostname> は Cisco Unified Service Monitor および Cisco Unified Operations Manager system のホスト名です。レジストリの変更後に **Daemon Manager** をリスタートして下さい。

ネットワーク内のシスコ デバイスに適用可能な対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Mitigation Bulletin』にて参照できます。
http://www.cisco.com/warp/public/707/cisco-amb-201100914-cusm-lms.shtml

修正済みソフトウェアの入手

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前にお客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

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、ご購入いただいたフィーチャ 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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項または、Cisco.com Downloads の http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他の条項に従うことに同意したことになります。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、シスコのワールドワイド Web サイト上の Software Center からアップグレードを入手することができます。 http://www.cisco.com

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、本脆弱性に関する適切な処置について指示と支援を受けてください。

回避策の効果は、使用製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品が多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

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 Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。TAC の連絡先は次のとおりです。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このお知らせの URL をご用意ください。サービス契約をご利用でないお客様に対する無償アップグレードは、TAC 経由でご要求いただく必要があります。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、 http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html を参照してください。

不正利用事例と公式発表

Cisco PSIRT では、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とその公表は確認しておりません。

これらの脆弱性は、AbdulAziz Hariri 氏によって発見され、ZDI からシスコに報告されたものです。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

本アドバイザリは、次のシスコのワールドワイド Web サイト上に掲載されます。

http://www.cisco.com/warp/public/707/cisco-sa-20110914-cusm.shtml

ワールドワイド Web 以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものもシスコのワールドワイド Web サイトに掲載される予定です。しかしながら、前述のメーリング リストもしくはニュースグループに対し積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最新情報をご確認いただくことをお勧めいたします。

更新履歴

Revision 1.1	2011-September-22	Updated workaround information
Revision 1.0	2011-September-14	Initial public release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、シスコ ワールドワイド Web サイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。このページには、シスコのセキュリティ通知に関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは http://www.cisco.com/go/psirt/ で確認することができます。