Cisco Unified Service MonitorおよびCisco Unified Operations Managerのリモートコード実行の脆弱性

アドバイザリーID : cisco-sa-20110914-cusm
初公開日 : 2011-09-14 16:00
最終更新日 : 2011-09-22 06:17
バージョン 1.1 : Final
回避策 : No Workarounds available
Cisco バグ ID :

概要

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、認証されていないリモートの攻撃者が該当サーバで任意のコードを実行する可能性があります。

シスコはこれら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。

これら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、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110914-cusm で公開されています。

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に関する個別のアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110914-lmsから入手できます。

該当製品

脆弱性のある製品

Cisco Unified Service MonitorおよびCisco Unified Operations Managerの8.6より前のすべてのバージョンが影響を受けます。

Cisco Unified Service MonitorおよびCisco Unified Operations Managerのソフトウェアバージョンを確認するには、Administration > Software Center (Common Services) > Software Updateの順に選択します。Software Updateページには、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。

脆弱性を含んでいないことが確認された製品

CiscoWorks LAN Management Solution以外のシスコ製品においてこの脆弱性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の製品です。Cisco Unified Communications Systemでサポートされるアクティブコールを継続的に監視する方法を提供します。

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、認証されていないリモートの攻撃者が該当サーバで任意のコードを実行する可能性があります。これらの脆弱性は、TCPポート9002を介して該当サーバに一連の巧妙に細工されたパケットを送信することによって引き起こされます。

これらの脆弱性はどちらもCisco Bug ID CSCtn42961 (登録ユーザ専用)として文書化され、CVE IDとしてCVE-2011-2738が割り当てられています。

回避策

DMFブローカと同じシステム上でこれらのアプリケーションが実行されているCisco Unified Service MonitorまたはCisco Unified Operations Managerのインストールでは、回避策として、管理者は次のレジストリキーを変更できます。

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システムのホスト名です。レジストリの更新後にDaemon Managerを再起動します。

ネットワーク内のCiscoデバイスに配備できる緩和策については、このアドバイザリに関連するCisco適用対応策速報を参照してください。http://www.cisco.com/warp/public/707/cisco-amb-201100914-cusm-lms.shtml

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照し

て、問題の解決状況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。

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、次のリンクからダウンロードできます。

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

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

これらの脆弱性は、ZDIによってシスコに報告され、AbdulAziz Haririによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110914-cusm

改訂履歴

リビジョン 1.1	2011年9月22日	回避策の情報を更新。
リビジョン 1.0	2011年9月14日	初版リリース

利用規約

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。