CiscoWorks LAN Management Solutionにおけるリモートコード実行の脆弱性

アドバイザリーID : cisco-sa-20110914-lms
初公開日 : 2011-09-19 15:30
最終更新日 : 2011-10-19 20:30
バージョン 1.2 : Final
回避策 : No Workarounds available
Cisco バグ ID :

概要

CiscoWorks LAN Management Solution(LMS)ソフトウェアには2つの脆弱性があり、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はありません。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110914-lms で公開されています。

注： Cisco Unified Service MonitorおよびCisco Unified Operations Managerもこれらの脆弱性の影響を受けます。Cisco Unified Service MonitorおよびCisco Unified Operations Managerに関するアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110914-cusmから入手できます。

該当製品

脆弱性のある製品

CiscoWorks LAN Management Solutionソフトウェアリリース3.1、3.2、および4.0は、この脆弱性の影響を受けます。

Cisco LAN Management Solution(LMS)バージョン3.1および3.2は、Device Fault Managementコンポーネント(DFM)がインストールされている場合にのみ脆弱です。Cisco

LAN Management Solutionバージョン4.0には、インストール時に選択されたオプションに関係なく脆弱性が存在します。

注： Cisco Unified Service MonitorおよびCisco Unified Operations Managerもこれらの脆弱性の影響を受けます。

脆弱性を含んでいないことが確認された製品

Cisco Unified Service MonitorおよびCisco Unified Operations Manager以外のシスコ製品で、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

CiscoWorks LAN Management Solutionは、ネットワークの設定、管理、監視、およびトラブルシューティングを簡素化する管理機能の統合スイートです。

CiscoWorks LAN Management Solution(LMS)ソフトウェアには2つの脆弱性があり、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。

注：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。

両方の脆弱性は、Cisco Bug ID CSCtn64922 (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

これらの脆弱性を軽減する回避策はありません。

ネットワーク内のCiscoデバイスに適用可能な他の対応策は、このアドバイザリに関連するCisco適用対応策速報を次のリンク先で参照できます。
http://www.cisco.com/warp/public/707/cisco-amb-201100914-cusm-lms.shtml

修正済みソフトウェア

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 Prime LAN Management Solutionソフトウェアバージョン4.1、およびCiscoWorks LAN Management Solutionの3.2.1および4.0.1サービスパックリリースで修正されて

います。

Cisco Prime LAN Management Solution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=283427841&i=rm

CiscoWorks LAN Management Solution 4.0.xのパッチは、次のリンクからダウンロードできます。

- Windowsの場合：http://www.cisco.com/cisco/software/release.html?mdfid=283434800&flowid=19062&softwareid=2
- Solarisの場合：http://www.cisco.com/cisco/software/release.html?mdfid=283434800&flowid=19062&softwareid=2

CiscoWorks LAN Management Solution 3.2のパッチは、次のリンクからダウンロードできます。

- Windowsの場合：http://www.cisco.com/cisco/software/release.html?mdfid=282635181&flowid=16561&softwareid=2
- Solarisの場合：http://www.cisco.com/cisco/software/release.html?mdfid=282635181&flowid=16561&softwareid=2

推奨事項

$propertyAndFields.get("recommendations")

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やその公表は確認しておりません。

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-lms

改訂履歴

リビジョン 1.2	2011年10月19日	「脆弱性スコア詳細」セクションの表のタイトルを更新

リビジョン 1.1	2011年9月17日	「ソフトウェアバージョンと修正」セクションを更新
リビジョン 1.0	2011年9月14日	初版リリース

利用規約

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。

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。