Cisco Prime LAN Management Solutionのコマンド実行の脆弱性

アドバイザリーID : cisco-sa-20130109-lms CVE-2012-6392
初公開日 : 2013-01-09 16:00
最終更新日 : 2013-01-23 20:31
バージョン 1.1 : Final
CVSSスコア : 10.0
回避策 : No Workarounds available
Cisco バグ ID : CSCuc79779

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 Prime LAN Management Solution(LMS)仮想アプライアンスには、認証されていないリモートの攻撃者がrootユーザの権限で任意のコマンドを実行できる可能性のある脆弱性が存在します。この脆弱性は、特定のTCPポートに送信される認証および許可コマンドの検証が不適切であることに起因します。攻撃者は、該当システムに接続して任意のコマンドを送信することにより、この脆弱性を不正利用する可能性があります。

シスコはこ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。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130109-lms

該当製品

脆弱性のある製品

LinuxベースのCisco Prime LMS仮想アプライアンスの次のバージョンには脆弱性が存在します。

Cisco Prime LMS仮想アプライアンスバージョン	該当
4.1	Yes
4.2	Yes
4.2.1	Yes

4.2.2	Yes
4.2.3	いいえ

注： この脆弱性の影響を受けるのは、LinuxベースのCisco Prime LMS仮想アプライアンスのみです。WindowsまたはSolaris上で動作するCisco Prime LMSは影響を受けません。

脆弱性を含んでいないことが確認された製品

次の製品は、この脆弱性の影響を受けません。

- Windows向けCisco Prime LMS
- Solaris向けCisco Prime LMS
- サポートされているオペレーティングシステム上で動作するCiscoWorks LMS

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 Prime LAN Management Solution(LMS)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。Cisco Prime LMSソフトウェアは、WindowsおよびSolarisでサポートされるか、仮想アプライアンスモード（ソフトアプライアンスモードとも呼ばれる）で配布されます。

Cisco Prime LMS仮想アプライアンスは、Linuxベースのオペレーティングシステム(OS)とプリインストールされたLMSアプリケーションのバンドルです。このソフトウェアは、サポートされているVMware仮想化環境で直接インスタンス化できる単一のOpen Virtual Archive(OVA)ファイルで配布されます。

LinuxベースのCisco Prime LAN Management Solution(LMS)仮想アプライアンスには、認証されていないリモートの攻撃者がrootユーザの権限で任意のコマンドを実行できる可能性のある脆弱性が存在します。この脆弱性は、該当システムで実行されているリモートシェルサーバ(rshd)による認証および許可コマンドの検証が不適切なことに起因します。攻撃者は、該当システムのリモートシェル(rsh)サービスにアクセスし、任意のコマンドを送信することで、この脆弱性を不正利用する可能性があります。

注：この脆弱性の影響を受けるのは、LinuxベースのCisco Prime LMS仮想アプライアンスのみです。WindowsまたはSolaris上で動作するCisco Prime LMSは影響を受けません。

この脆弱性は、TCP ポート 514 経由で悪用される可能性があります。

この脆弱性は、Cisco Bug ID CSCuc79779(登録ユーザ専用)として文書化され、CVE IDとして

CVE-2012-6392が割り当てられています。

回避策

この脆弱性を回避するには、管理者が該当システムの /etc/ディレクトリに保存されている securettyファイルを編集して、 rshサービスのコマンドラインを削除する必要があります。

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 Intelligence』にて参照できます。
https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=27920

修正済みソフトウェア

次の表に、このセキュリティアドバイザリに記載された脆弱性を緩和するためのソフトウェアアップグレード情報を示します。

Cisco Prime LMS仮想アプライアンスバージョン	パッチ名
4.1	lms4.1-lnx-CSCuc79779-0.zip
4.2	lms4.2-lnx-CSCuc79779-0.zip
4.2.1	lms4.2.1-lnx-CSCuc79779-0.zip
4.2.2	lms4.2.2-lnx-CSCuc79779-0.zip

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性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規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、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。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（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。この脆弱性の不正利用を示す機能コードは、Metasploitフレームワークの一部として使用できます。

この脆弱性は、サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130109-lms

改訂履歴

リビジョン 1.1	2013年1月23日	概要、詳細、回避策、エクスプロイト事例、公式発表のセクションを更新
リビジョン 1.0	2013年1月9日	初版リリース

利用規約

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。