複数のシスコ製品におけるルートシェルアクセスの脆弱性

Medium

アドバイザリーID : Cisco-SA-20130219-CVE-2013-1125 CVE-2013-1125
初公開日 : 2013-02-19 18:28
バージョン 1.0 : Final
CVSSスコア : 6.8
回避策 : No Workarounds available
Cisco バグ ID : CSCud95790 CSCue46025 CSCue46058 CSCue46013 CSCue46035 CSCue46001 CSCue46023 CSCue46021 CSCue46031 CSCue46042 CSCue46049

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

複数のシスコ製品に、ローカルの攻撃者が root権限を使用してシェルアクセスを取得できる可能性のある脆弱性が存在します。

この脆弱性は、該当ソフトウェアを実行するシスコ製品のコマンドラインインターフェイス(CLI)で処理されるユーザ入力の検証が正しく行われないことに起因します。該当デバイスへのアクセス権を持つローカル攻撃者は、脆弱なコンポーネントによって処理される特別に巧妙に細工された入力を送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はターゲットシステムで ルート権限を使用してシェルアクセスを取得し、その結果、システム全体が侵害される可能性があります。

シスコはこの脆弱性を確認していますが、ソフトウェアアップデートは提供されていません。

この脆弱性をエクスプロイトするには、攻撃者がターゲットシステムにローカルアクセスできる必要があります。このアクセス制限により、エクスプロイトが成功する可能性が制限されます。

影響を受ける製品とバージョンの最新のリストについては、ベンダーアナウンスセクションのバグレポートを参照してください。

該当製品

シスコは、Bug ID CSCue46001、CSCud95790、CSCue46021、CSCue46025、CSCue46023、

CSCue46058、CSCue46013、CSCue4のセキュリティ通知をリリースしました6031、CSCue46035、およびCSCue46042(CVE-2013-1125)

脆弱性のある製品

このアラートが最初に公開された時点では、次のバージョンのシスコ製品に脆弱性が存在していました。シスコ製品の新しいバージョンも影響を受ける可能性があります。

- Cisco Identity Services Engine(ISE)ソフトウェアバージョン1.0.4.53以前
- Cisco Secure Access Control System(ACS)バージョン5.4以前
- Cisco Application Networking Manager(ANM)バージョン2.0アップデートA以前
- Cisco Prime LAN Management Solution(LMS)バージョン4.1以前
- Cisco Prime Network Control System(NCS)バージョン1.1以前
- Cisco Quadバージョン2.0
- Cisco Context Directory Agentバージョン1.0
- Cisco Prime Collaborationバージョン9.0
- Cisco Unified Provisioning Managerバージョン8.5
- Cisco Network Services Managerバージョン5.0.2以前

脆弱性を含んでいないことが確認された製品

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。

回避策

今後のアップデートやリリースについては、ベンダーに問い合わせることをお勧めします。

信頼できるユーザーだけがローカルシステムにアクセスできるようにすることを推奨します。

影響を受けるシステムを監視することを推奨します。

修正済みソフトウェア

ソフトウェアの更新プログラムは利用できません。

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）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を確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20130219-CVE-2013-1125

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2013年2月19日

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。