

Cisco MARSの情報漏えいの脆弱性

Medium	アドバイザーID : Cisco-SA-20130304-CVE-2013-1140	CVE-2013-1140
	初公開日 : 2013-03-04 21:24	
	バージョン 1.0 : Final	
	CVSSスコア : 4.3	
	回避策 : No Workarounds available	
	Cisco バグ ID : CSCue55093	

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 Security Monitoring, Analysis and Response System(MARS)のXMLパーサーの設定における脆弱性により、認証されていないリモートの攻撃者が、該当システムに保存されている情報の一部に「読み取り」アクセスする可能性があります。

この脆弱性は、XMLファイルを解析する際のXML外部エンティティ(XXE)の不適切な処理に起因します。攻撃者は、該当システムの管理者に巧妙に細工されたXMLファイルをインポートするように説得することで、この脆弱性を不正利用する可能性があります。成功するためには、攻撃者はCisco MARS管理IPアドレスから到達可能で、該当システムから送信された情報の取得に使用されるサーバを所有している必要があります。

シスコは脆弱性を確認しましたが、ソフトウェアアップデートは利用できません。

不正利用に成功するには、該当システムから送信された情報を取得するために使用される該当ソフトウェアIPアドレスを実行しているデバイスから到達可能なサーバを攻撃者が所有している必要があります。この目的を達成するには、攻撃者が信頼できる内部ネットワークにアクセスする必要があります。このアクセス要件により、不正利用が成功する可能性が低くなります。

影響を受けるバージョンの最新のリストについては、ベンダー発表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、[CVE-2013-1140](#)のリンクで、バグID [CSCue55093](#)のセキュリティ通知をリリースしました。

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、Cisco MARSバージョン6.0.4以前には脆弱性が存在していました。Cisco MARSの新しいバージョンも影響を受ける可能性があります。

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、ベンダーに連絡することを推奨します。

IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけに該当システムへのアクセスを許可することを検討することもできます。

未承諾の電子メールの添付ファイルを開かないよう推奨します。添付ファイルを開く前に、ファイルが安全であることを確認する必要があります。

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。

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-20130304-CVE-2013-1140>

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3月4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。

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、単独の転載や意識を施した場合、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。