Cisco Connected Grid Network Management Systemのクロスサイトスクリプティングの脆弱性

アドバイザリーID : Cisco-SA-20130401-CVE-2013-1171 CVE-2013-1171
初公開日 : 2013-04-01 20:35
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : No Workarounds available
Cisco バグ ID : CSCue38868 CSCue14517 CSCue38866 CSCue38914 CSCue38882 CSCue38872 CSCue38881 CSCue38853 CSCue38884 CSCue14540

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 Connected Grid Network Management System(CG-NMS)には、認証されていないリモートの攻撃者によるクロスサイトスクリプティング攻撃を可能にする可能性のある複数の脆弱性が存在します。

Cisco Connected Grid Network Management System(CGNS)は、エレメントリストコンポーネントのクロスサイトスクリプティング(XSS)の脆弱性の影響を受けやすくなっています。XSS攻撃では、Unicode方式を使用してタグまたはスクリプトの悪意のある部分をエンコードすることにより難読化を行うため、リンクまたはHTMLコンテンツがサイトを閲覧するエンドユーザに対して偽装されます。脆弱なサーバがユーザのブラウザに悪意のあるコードを注入するために使用されているため、トレースバック方式を使用して悪意のあるユーザの身元を隠し、XSS攻撃の原因を特定することは困難です。

シスコは、セキュリティ通知でこれらの脆弱性が確認されており、ソフトウェアアップデートが利用可能であることを確認しています。

この脆弱性を不正利用するために、攻撃者は悪意のあるサイトにユーザを誘導するリンクを提供し、誤解を招く言語または命令を使用して提供されたリンクに従うようにユーザを説得する可能性があります。

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。

シスコはCVSSスコアを通じて、機能的なエクスプロイトコードが存在することを示していますが、このコードが一般に公開されることは確認されていません。

該当製品

シスコは、Bug ID CSCue14517、CSCue38914、CSCue38884、CSCue38882、CSCue38881、CSCue38872、CSCue38868、CSCue3のセキュリティ通知をリリースしました8866、CSCue38853、およびCSCue14540(CVE-2013-1171)

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 CG-NMSバージョン1.0(42)以前には脆弱性が存在していました。Cisco CG-NMS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

適切なアップデートを適用することを推奨します。

不審な送信元や認識されていない送信元からの電子メールメッセージを開かないよう推奨します。電子メールメッセージに含まれるリンクや添付ファイルが安全かどうかをユーザーが確認できない場合は、開かないことをお勧めします。

クロスサイトスクリプティング攻撃と、この脆弱性を悪用するために使用される方法の詳細については、Cisco適用対応策速報『クロスサイトスクリプティング(XSS)の脅威ベクトルについて』を参照してください。

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

契約が有効なシスコのお客様は、シスコのサポートチームに連絡して、この脆弱性の修正を含むソフトウェアバージョンへのアップグレードの支援を受ける必要があります。契約をご利用でないお客様は、1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)にお問い合わせいただくか、 tac@cisco.comの電子メールでサポートを受けることができます。

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-20130401-CVE-2013-1171

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4月1日

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。