Cisco Application Control Engine AdministratorのIPアドレスのオーバーラップに関する脆弱性

High

アドバイザリーID : cisco-sa-20120620-ace CVE-2012-3063
初公開日 : 2012-06-20 16:00
最終更新日 : 2012-06-20 19:27
バージョン 1.1 : Final
CVSSスコア : 7.1
回避策 : No Workarounds available
Cisco バグ ID : CSCts30631

概要

Cisco Application Control Engine(ACE)ソフトウェアに脆弱性が存在します。 管理ユーザがマルチコンテキストモードで実行されている場合、ACEの意図しないコンテキスト（仮想インスタンス）にログイン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-20120620-ace

該当製品

脆弱性のある製品

Cisco ACEアプライアンスまたはモジュールは、マルチコンテキストモードで稼働している場合に脆弱です。 この脆弱性を不正利用するには、2つ以上のコンテキストを同じ管理IPアドレスで設定する必要があります。 管理者が意図したコンテキストの管理IPアドレスにアクセスしようとすると、意図したコンテキストとは異なるコンテキストにログインする可能性があります。管理者は、意図しないコンテキストに対する有効なログインクレデンシャルを持っている必要があります。そうしないと、アクセスが拒否されます。

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。

詳細

Cisco ACEアプライアンスまたはモジュールは、マルチコンテキストモードで稼働している場合に脆弱です。 この脆弱性を不正利用するには、2つ以上のコンテキストを同じ管理IPアドレスで設定する必要があります。管理者は、ログイン時に正しくないコンテキストに対する有効なログインクレデンシャルを持っている必要があります。

この脆弱性は、Cisco Bug ID CSCts30631(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2012-3063が割り当てられています。

回避策

Cisco ACEの各コンテキストに一意の管理IPアドレスを設定します。設定に関するリファレンスは次のリンクから入手できます。
http://www.cisco.com/en/US/partner/docs/app_ntwk_services/data_center_app_services/ace_appliances/v

修正済みソフトウェア

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。

この脆弱性は、Cisco ACEソフトウェアバージョンA4(2.3)およびA5(1.1)で修正されています。これらのソフトウェアバージョンは、Cisco Software Navigator(http://www.cisco.com/cisco/software/navigator.html)からACEアプライアンスおよびACEモジュールの両方で使用できます。

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。

この脆弱性は、お客様のケースのトラブルシューティング中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ace

改訂履歴

リビジョン 1.1	2012年6月20日	修正されたCVE ID
リビジョン 1.0	2012年6月20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。