Cisco Prime Data Center Network Managerのリモートコマンド実行の脆弱性

アドバイザリーID : cisco-sa-20121031-dcnm
初公開日 : 2012-10-31 16:00
最終更新日 : 2013-05-08 16:00
バージョン 2.0 : Final
CVSSスコア : 10.0
回避策 : No Workarounds available
Cisco バグ ID : CSCua31204 CSCtz44924

CVE-2012-5417

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 Data Center Network Manager(DCNM)にはリモートコマンド実行の脆弱性があり、認証されていないリモートの攻撃者が、Cisco Prime DCNMアプリケーションを実行しているコンピュータ上で任意のコマンドを実行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-20121031-dcnm

注：このアドバイザリが最初に公開された後、DCNMソリューションの一部であるDCNM SANサーバコンポーネントに加え、DCNM LANサーバも同じ脆弱性の影響を受けることが判明しました。このアドバイザリはリビジョン2.0に更新され、DCNM LANサーバコンポーネントにも脆弱性があることが示されています。また、DCNM LANサーバコンポーネントの脆弱性を追跡するCisco Bug IDが提供され、修正済みソフトウェア情報が更新されています。

該当製品

脆弱性のある製品

Microsoft WindowsおよびLinuxプラットフォーム向けのCisco Prime Data Center Network Manager(DCNM)の6.1(2)より前のリリースはすべて、この脆弱性の影響を受けます。Cisco

Prime DCNMソリューションに含まれるCisco DCNM-LANサーバとCisco DCNM-SANサーバは、両方ともこの脆弱性の影響を受けます。

注：Cisco DCNM-LANサーバとCisco DCNM-SANサーバは、リリース6.1(1)で単一のCisco Prime DCNM製品に統合されるまで異なる製品でした。Cisco DCNM-LANサーバおよびCisco DCNM-SANのすべてのリリースがこの脆弱性の影響を受けます。

実行中の Cisco Prime DCNM リリースを確認するには、管理者が Web ブラウザと HTTPS を使用して Cisco Prime DCNM ソフトウェアを実行するコンピュータに接続してください。ログインする前に、ログインページにリリース番号が表示されます。次の例は、バージョン6.1(1a)を実行しているデバイスを示しています。

```
Cisco Prime
Data Center Network Manager
Version: 6.1(1a)
```

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 Prime DCNM（旧製品名：Cisco Data Center Network Manager）は、イーサネットとストレージネットワークの管理を 1 つのダッシュボードに統合するネットワーク管理アプリケーションです。このアプリケーションを使用すると、ネットワークとストレージの管理者は、Cisco NX-OS ソフトウェアを実行するさまざまなシスコ製品ファミリの正常性とパフォーマンスを管理およびトラブルシュートできます。

6.1(2)より前のバージョンを実行するCisco Prime DCNM（Cisco DCNM-LANサーバおよびCisco DCNM-SANサーバコンポーネント）には、Cisco Prime DCNMアプリケーションをホストするオペレーティングシステム上で、認証されていないリモートの攻撃者が任意のコマンドを実行できる脆弱性が存在します。

この脆弱性は、JBoss Application Server Remote Method Invocation(RMI)サービス、特にjboss.system:service= MainDeployer機能が不正なユーザにさらされるために存在します。認証されていないリモートの攻撃者が、RMIサービス経由で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。この不正利用により、攻撃者はデバイス上で任意のコマンドを実行できる可能性があります。

コマンドは、Microsoft Windows上で動作するCisco Prime DCNMの Systemユーザまたは Linux上で動作するCisco Prime DCNMの rootユーザのコンテキストで実行されます。

Cisco Prime DCNMは、RMIレジストリ機能にTCPポート1099または9099を使用します（Cisco

Prime DCNMのバージョンによって異なります）。RMIトランザクションは、常にRMIレジストリポートへのTCP接続で開始されます。

この脆弱性は、Cisco DCNM-SANサーバおよびCisco DNCM-LANサーバコンポーネントに関して、それぞれCisco Bug ID CSCtz44924(登録ユーザ専用)および CSCua31204(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が割されています。7.

回避策

RMIトランザクションはRMIレジストリポートへの接続から始まります。RMIレジストリポートは、Cisco Prime DCNMのバージョンに応じてデフォルトでTCPポート1099または9099です。そのため、正当なデバイスだけがRMIレジストリポートに接続できるようにすることで、この脆弱性を軽減できます。

ネットワーク内のシスコデバイスに適用可能な他の対応策は、次のリンクにある付属ドキュメント『Identifying and Mitigating Exploitation of the Cisco Prime Data Center Network Manager Remote Command Execution Vulnerability』で参照できます。

https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=27268

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 のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の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 Prime Data Center Network Managerリリース6.1(2)で最初に修正されています。

Cisco Prime Data Center Network Managerは、Cisco.comのSoftware Centerからダウンロードできます。 http://www.cisco.com/cisco/software/navigator.htmlにアクセスし、 製品>クラウドおよびシステム管理>データセンターインフラストラクチャ管理> Cisco Prime Data Center Network Managerの順に選択してください。

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は確認しておりません。

Metasploitフレームワークには、この脆弱性の原因となったJBoss設定を不正利用するエクスプロイトモジュール(Jboss_maindeployer)があります。

この脆弱性は、Security Compass(www.securitycompass.com)のPaul O'Grady氏によってシスコに報告されました。シスコは、この脆弱性を報告いただき、弊社と連携しての公開にご協力いただいたO'Grady氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121031-dcnm

改訂履歴

Revision 2.0	2013年5月8日	DNCMのDCNM LANサーバコンポーネントもこの脆弱性の影響を受けることを示すアドバイザリを更新。対応するCisco Bug ID CSCua31204を追加し、修正済みソフトウェアを更新。
リビジョン 1.0	2012年10月31日	初回公開リリース

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。