Multiple Vulnerabilities in Cisco Prime Data Center Network Manager

Advisory ID: cisco-sa-20130918-dcnm

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130918-dcnm

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。

Revision 1.0

For Public Release 2013 September 18 16:00 UTC (GMT)

目次

要約

Cisco Prime Data Center Network Manager（DCNM）には、リモートの攻撃者によって、該当デバイスのファイルのコンポーネントが開示されテキスト ファイルにアクセスされる可能性のある複数の脆弱性が存在します。Cisco Prime DCNM の複数のコンポーネントがこの影響を受けます。これらの脆弱性は同一のデバイスで個別に不正利用される可能性があります。ただし、1 つの脆弱性に影響を受けるリリースが、その他の脆弱性からも影響を受けるとは限りません。

Cisco Prime DCNM は次の脆弱性の影響を受けます。

- Cisco Prime DCNM の情報開示に関する脆弱性
- Cisco Prime DCNM のリモートからのコマンド実行の脆弱性
- Cisco Prime DCNM の XML 外部エンティティ インジェクションの脆弱性

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。現在、これらの脆弱性を軽減する回避策はありません。このアドバイザリは、次のリンクで確認で

きます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130918-dcnm

該当製品

脆弱性が認められる製品

次の製品は、このアドバイザリに記載される脆弱性の影響を受けます。

- Cisco Prime Data Center Network Manager（DCNM）4.1
- Cisco Prime Data Center Network Manager（DCNM）4.2
- Cisco Prime Data Center Network Manager（DCNM）5.0
- Cisco Prime Data Center Network Manager（DCNM）5.1
- Cisco Prime Data Center Network Manager（DCNM）5.2
- Cisco Prime Data Center Network Manager（DCNM）6.1

脆弱性が認められない製品

他のシスコ製品においてこの脆弱性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（旧名称 Cisco Data Center Network Manager）は、イーサネットおよびストレージ ネットワークの管理を単一のダッシュボードに結合したネットワーク管理アプリケーションであり、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健全性とパフォーマンスをネットワーク管理者およびストレージ管理者が管理およびトラブルシューティングするために役立ちます。

Cisco Prime DCNM の情報開示に関する脆弱性

Cisco Prime DCNM の Cisco DCNM-SAN Server コンポーネントには、認証されていないリモートの攻撃者によって該当システムの任意のファイル コンテンツが開示される可能性のある脆弱性が存在します。

この脆弱性は Cisco Bug ID CSCue77029（登録ユーザ専用）として文書化され、CVE ID として CVE-2013-5487 が割り当てられています。

Cisco Prime DCNM のリモートからのコマンド実行の脆弱性

Cisco Prime DCNM の Cisco DCNM-SAN Server コンポーネントには 2 つの脆弱性があり、認証されていないリモートの攻撃者によって、Cisco Prime DCNM アプリケーションをホストする基盤のオペレーティング システムで任意のコマンドが実行される可能性があります。

コマンドは、Cisco Prime DCNM が Microsoft Windows で稼働している場合は System ユーザとして、Linux で稼働している場合は root ユーザとして実行されます。

これらの脆弱性は、Cisco Bug ID CSCue77035（登録ユーザ専用）および CSCue77036（登録ユーザ専用）として文書化され、CVE ID として CVE-2013-5486 が割り当てられています。

Cisco Prime DCNM の XML 外部エンティティ インジェクションの脆弱性

Cisco Prime DCNM は、認証されていないリモートの攻撃者が XML 外部エンティティ インジェ

クション攻撃を使用して、基盤となるオペレーティング システム上の任意のテキスト ファイルに root 権限でアクセスできる可能性のある脆弱性が存在します。このようなアクセス要求、XML 外部エンティティの参照、挿入されたタグが処理されると、情報が開示されてしまう場合があります。

この脆弱性は、Cisco Bug ID CSCud80148（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-5490 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCue77029 - Cisco Prime DCNM Information Disclosure Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	None	None
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCue77035 - Cisco Prime DCNM Remote Code Execution Vulnerability

Calculate the environmental score of					
CVSS Base Score - **10.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **8.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCue77036 - Cisco DCNM Remote Code Execution Vulnerability Calculate the environmental score of					
CVSS Base Score - **10.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **8.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCud80148 - Cisco Prime DCNM XML External Entity Injection Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	None	None
CVSS Temporal Score - **6.8**					
Exploitability		Remediation Level		Report Confidence	
High		Official-Fix		Confirmed	

影響

Cisco Prime DCNM のリモートからのコマンド実行の脆弱性

リモートからのコマンド実行の脆弱性が不正利用されると、認証されていないリモートの攻撃者は、Cisco Prime DCNM が Microsoft Windows で稼働している場合は System ユーザとして、または Linux で稼働している場合は root ユーザとして、Cisco Prime DCNM アプリケーションをホストする基盤のオペレーティング システム上で任意のコマンドを実行できる可能性があります。

Cisco Prime DCNM の情報開示に関する脆弱性

情報開示に関する脆弱性の不正利用に成功した場合、認証されていないリモートの攻撃者が該当システムの任意のファイル コンテンツを開示できる可能性があります。

Cisco Prime DCNM の XML 外部エンティティ インジェクションの脆弱性

XML 外部エンティティ インジェクションの脆弱性の不正利用に成功した場合、認証されていないリモートの攻撃者が該当システムの任意のファイル コンテンツを閲覧できる可能性があります。

ソフトウェア バージョンおよび修正

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, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

Cisco Bug ID CSCue77035（ 登録ユーザ専用 ）の脆弱性は、Cisco Prime DCNM バージョン 6.2(2) で修正されています。
このアドバイザリに記載されているその他の脆弱性は、Cisco Prime DCNM バージョン 6.2(3) で修正されています。

次のリンク先から、最新バージョンの Cisco Data Center Network Manager をダウンロードできます。
http://software.cisco.com/download/release.html?mdfid=281722751&softwareid=282088134&release=6.2%283%29&relind=AVAILABLE&rellifecycle=&reltype=latest&i=rm

Cisco Prime DCNM は、Cisco.com 内の Software Center（http://www.cisco.com/cisco/software/navigator.html ）にアクセスし、 **[Products] > [Cloud and Systems Management] > [Data Center Infrastructure Management] > [Cisco Prime Data Center Network Manager]** からダウンロードできます。

回避策

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、このアドバイザリの付属ドキュメントである『Cisco Applied Intelligence』にて参照できます。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=30682

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレードを入手することができます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

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とその公表は確認しておりません。

Cisco Prime DCNM のリモートからのコマンド実行の脆弱性と情報開示の脆弱性は、TippingPoint 社の Zero Day Initiative（ZDI）からシスコに報告されました。

Cisco Prime DCNM の XML 外部エンティティ インジェクションの脆弱性は、Ben Williams 氏と NCC Group から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ことに対して、各機関に感謝いたします。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130918-dcnm

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2013-September-18	Initial public release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。