Cisco Prime Network Control Systems Database Default Credentials Vulnerability

Advisory ID: cisco-sa-20130410-ncs

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130410-ncs/

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 1.1

Last Updated 2013 July 2 16:03 UTC (GMT)

For Public Release 2013 April 10 16:00 UTC (GMT)

目次

要約

バージョン 1.1.1.24 より前のソフトウェアを実行している Cisco Prime Network Control System NCS アプライアンスには、デフォルトのクレデンシャルで作成されたデータベース ユーザ アカウントが含まれます。攻撃者がこのアカウントを使用して、アプリケーション構成を変更したり、サービスを中断させたりする可能性があります。

この脆弱性を解決するにはソフトウェアのアップグレードが必要です。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。この脆弱性に対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-20130410-ncs/

該当製品

脆弱性が認められる製品

1.1.1.24 より前のバージョンの Cisco Prime Network Control System

インストールおよび、接続されている Cisco Prime NCS のバージョンを確認するには、[Help] > [About Cisco NCS] からソフトウェア リリースを確認します。インストールされている Cisco Prime NCS のバージョンの詳細については、『 Cisco Prime Network Control System Configuration Guide, Release 1.1』を参照してください 。

脆弱性が認められない製品

この脆弱性の影響を受･ッる他のシスコ製品は、現在確認されていません。

詳細

Cisco Prime Infrastructure バンドルの一部である Cisco Prime（NCS）は、有線またはワイヤレスのネットワークにおける、ユーザ、アクセスおよび ID の統合管理を実現します。Cisco Prime NCS は、ブランチ ネットワークの導入と管理にも重点を置いた、シスコのワイヤレス LAN の包括的なライフサイクル管理機能を提供します。

Cisco Prime NCS にはデータベース ユーザ向けのデフォルト クレデンシャルが含まれます。リモートの攻撃者がデフォルト クレデンシャルを使用してデバイスの構成設定を変更したり、サービスを中断させたりする可能性があります。

この脆弱性は、Cisco Bug ID CSCtz30468（ 登録ユーザ専用）および CSCub54624（ 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-2013-1170 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、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/

CSCtz30468 - Cisco Prime Network Control System Default Credentials for Database User Calculate the environmental score of					
CVSS Base Score - **7.5**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	Partial	Partial
CVSS Temporal Score - **6.2**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCub54624 - Cisco Prime Network Control System Default Credentials Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.5**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	Partial	Partial
CVSS Temporal Score - **6.2**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

こ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 ユーザがデフォルト クレデンシャルを使用してデバイスの構成設定を変更したり、サービスを中断させたりす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 NCS リリース 1.1.1.24 は Cisco.com 内の Software Center からダウンロードできます。http://www.cisco.com/cisco/software/navigator.html 次のパスを使用してファイルにアクセスできます。

[Products] > [Wireless] > [Wireless LAN Management] > [Network Control System] > [Cisco Prime Network Control System Cisco Prime Network Control System 1.1] > [Prime Network Control System Virtual Appliance Software - NCS 1.1.1]

Cisco NCS リリース 1.1.1.24 はインストール中に、既存のデータベースのデフォルト クレデンシャルを削除します。

回避策

この脆弱性に対する回避策はありません。

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=28796/

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 ソフトウェアを入手できます。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。

多言語による各地の電話番号、説明、E メール アドレスなどの TAC の連絡先情報については、Cisco Worldwide Contact を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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。

この脆弱性は、Amazon の Erik Parker 氏によってシスコに報告されました。

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-20130410-ncs/

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 1.1	2013-July-02	Added CSCub54624; updated fixed version to 1.1.2 and above
Revision 1.0	2013-April-10	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。シスコ セキュリティ アドバイザリについては、すべて http://www.cisco.com/go/psirt/ で確認できます。