Cisco Security Advisory: Default Credentials Vulnerability in Cisco Network Registrar

Advisory ID: cisco-sa-20110601-cnr

http://www.cisco.com/warp/public/707/cisco-sa-20110601-cnr.shtml

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 2011 June 01 1600 UTC (GMT)

目次

要約

Cisco Network Registrar ソフトウェアの 7.2 より前のリリースには、管理者アカウント用のデフォルト パスワードが含まれています。最初のインストール中にユーザはこのパスワードの変更を強制されないため、インストール後も継続使用されることがあります。この脆弱性に気付いた攻撃者が管理者権限で認証を受け、Cisco Network Registrar の構成を任意に変更できる可能性があります。

ソフトウェア リリース 7.2 へのアップグレードは無料ではありませんが、このドキュメントで説明する回避策によって、この脆弱性の不正利用を阻止することができます。

ソフトウェア リリース 7.2 へのアップグレード時には、この回避策を使用して管理者アカウントのパスワードを変更する必要があります。Cisco Network Registrar のソフトウェア リリース 7.2 を新たにインストールする場合のみ、 新しい管理者パスワードの入力を要求されます。

この脆弱性の回避策は、「回避策」のセクションに記載された方法を使用して、管理者アカウントに関連付けられたパスワードを変更することです。

このアドバイザリは次のリンクに掲載されます。 http://www.cisco.com/warp/public/707/cisco-sa-20110601-cnr.shtml

該当製品

脆弱性が存在する製品

この脆弱性に該当するのは、ソフトウェア リリース 7.2 より前のすべての Cisco Network Registrar です。この脆弱性はあらゆるプラットフォーム上で稼働する該当リリースに存在します。

稼動している Cisco Network Registrar を確認するには、メニューから [About] オプションを選択するか、コマンドライン インターフェイスを使用して次のコマンドを実行します。

```
nrcmd> session get version
```

脆弱性が存在しない製品

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 Network Registrar は、拡張性と信頼性の高い DNS、DHCP、TFTP サービスを提供します。Cisco Network Registrar の中央管理機能により、ネットワークおよびデバイス構成に関連する管理タスクが簡素化されます。

Cisco Network Registrar には管理者アカウント用のデフォルト パスワードが含まれており、攻撃者はこのことを利用して管理者権限で認証を受け、Cisco Network Registrar の構成を任意に変更することが可能になります。この脆弱性は Cisco Bug ID CSCsm50627 （ 登録ユーザのみ ）に文書化されており、Common Vulnerabilities and Exposures（CVE）ID として CVE-2011-2024 が割り当てられています。

また、定期的にパスワードを変更することが推奨されます。変更の頻度は組織のセキュリティ ポリシーに従う必要がありますが、 ガイドラインとして、パスワードは年に 2、3 回変更する必要があります。これは 製品がいつインストールされたかを問わず、 あらゆる製品、ユーザ、管理者、そして管理者以外にも適用されます。

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。このセキュリティ 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手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（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、個々のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次のリンクにて CVSS に関する FAQ を提供しています。

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

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを以下の URL にて提供しています。

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

Initially supplied admin password not changed during the installation **Calculate the environmental score of**					
CVSS Base Score - **10**					
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	

影響

この脆弱性の不正利用に成功した場合、攻撃者は Cisco Network Registrar の構成を任意に変更できるようになります。

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際には、 http://www.cisco.com/go/psirt/ および本アドバイザリ以降に公開のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が不明確な場合は、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、ソフトウェア リリース 7.2 で修正されています。7.2 より前のすべての Cisco Network Registrar は、最初のインストール中に管理者パスワードの変更をユーザに強制しません。

回避策

管理者アカウントに関連付けられたパスワードを変更することが回避策となります。Web インターフェイスを使用してパスワードを変更するには、 メニューから **[Advanced] -> [Administrators] -> [Admin]** を選択します。

コマンドライン インターフェイスを使用する場合は次のコマンドを実行し、管理者のパスワードを変更します。

```
nrcmd> session get version
```

また、Cisco Network Registrar（TCP ポート 8080、8090、8443、8453）と、それが稼動しているホストへのアクセスは、正当な IP アドレスのみに制限される必要があります。このタスクを実行するための詳細については、ホストのオペレーティング システムに関するドキュメントを参照してください。

認証の形式として IP アドレスを使用することは、ネットワーク セキュリティの方法として確立されているものです。アクセス コントロール リスト（ACL）の使用、またはデバイスおよびアプリケーションにおけるネットワーク管理ステーションの明確な識別についての詳細は、次のリンクにあるホワイト ペーパー『 A Security-Oriented Approach to IP Addressing』を参照してください。 http://www.cisco.com/web/about/security/intelligence/security-for-ip-addr.html

修正済みソフトウェアの入手

この脆弱性に対応するアップグレード ソフトウェアを無償で提供する予定はありません。このド

キュメントで説明されている回避策は、現在のリリースのソフトウェアでパスワードを変更する方法を示しています。

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 ライセンスの条項または、Cisco.com Downloads の http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他の条項に従うことに同意したことになります。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

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、シスコのワールドワイド Web サイト上の Software Center 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

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、本脆弱性に関する適切な処置について指示と支援を受けてください。

回避策の効果は、使用製品、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のお客様の状況に依存します。影響製品が多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

サービス契約をご利用でないお客様

シスコから直接購入したが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、サードパーティ ベンダーから購入したが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を入手してください。TAC の連絡先は次のとおりです。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

製品のシリアル番号とこの通知の URL をご用意ください。

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、 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 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。

この脆弱性は社内での確認中に発見されました。

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。またシスコシステムズ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

本アドバイザリは、次のシスコのワールドワイド Web サイト上に掲載されます。

http://www.cisco.com/warp/public/707/cisco-sa-20110601-cnr.shtml

ワールドワイド Web 以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- 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
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものもシスコのワールドワイド Web サイトに掲載される予定です。 しかしながら、前述のメーリング リストもしくはニュースグループに対し積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最新情報をご確認いただくことをお勧めいたします。

更新履歴

Revision 1.0	2001-06-01	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支援、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について詳しく知るには、シスコ ワールドワイド Web サイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。このページには、シスコのセキュリティ通知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。