Cisco Network Admission Control Manager SQL Injection Vulnerability

Advisory ID: cisco-sa-20130417-nac

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130417-nac/

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 April 17 16:00 UTC (GMT)

目次

要約

Cisco Network Admission Control（NAC）Manager には脆弱性が存在するため、認証されていないリモートの攻撃者が任意のコードを実行して該当システムの制御権を取得する可能性があります。攻撃に成功した場合、認証されていない攻撃者が NAC Manager データベースのあらゆる情報に対してアクセス、作成、または変更を行うことができるようになる可能性があります。

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-20130417-nac/

該当製品

脆弱性が認められる製品

下記のバージョンよりも前の Cisco NAC Manager がこの脆弱性の影響を受けます。

- 4.9.2
- 4.8.3.1

NAC Manager システムのソフトウェア バージョンを調べるには、管理インターフェイスで [Administration] > [CCA Manager] > [Software Upload | Current Version] の順に選択します。
ソフトウェアのバージョンは、Command Line Interface (CLI; コマンドライン インターフェイス) で **cat /perfigo/build** コマンドを実行して確認することもできます。

次の例は、該当するバージョン (4.9.1) のソフトウェアを実行しているシステムを示しています。

```
[root@nacmanager ]# cat /perfigo/build
VERSION=4.9.1
NAME=Clean Access Manager.
```

注： Cisco NAC Manager は Cisco NAC アプライアンス (旧称 Cisco Clean Access) の一部です。ソフトウェア バージョン 4.1.3 以降は Cisco Network Admission Control (NAC) の名称を使用しています。

脆弱性が認められない製品

Cisco NAC Manager を除いて、この脆弱性の影響を受けるシスコ製品は確認されていません。

注： Cisco NAC アプライアンス製品の Csco NAC サーバおよび NAC エージェント コンポーネントはこの脆弱性の影響を受けません。

詳細

Cisco NAC アプライアンス ソリューションを使用すると、ネットワーク管理者はユーザにネットワークへの接続を許可する前に、有線、ワイヤレス、およびリモートのユーザとそのマシンに対する認証、認可、評価、対策を行うことができます。このソリューションでは、マシンのネットワークへのアクセスを許可する前に、そのマシンがセキュリティ ポリシーに準拠しているかを確認し、脆弱性を修正します。

Cisco NAC Manager には脆弱性が存在するため、認証されていないリモートの攻撃者が任意のコードを実行して該当システムの制御権を取得する可能性があります。

この脆弱性は、ユーザからのリクエストに対する Cisco NAC Manager による検証が不適切であることに起因します。攻撃者は Structured Query Language (SQL) コマンドをインジェクションすることで、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、攻撃者は任意のクエリを実行して、該当システムの制御権を取得する可能性があります。

この脆弱性は、CSCub23095（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-2013-1177 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/

<table>
<tr><th colspan="6">CSCub23095-- Cisco NAC Manager SQL Injection Vulnerability
Calculate the environmental score of</th></tr>
<tr><td colspan="6">CVSS Base Score - 10.0</td></tr>
<tr><td>Access Vector</td><td>Access Complexity</td><td>Authentication</td><td>Confidentiality Impact</td><td>Integrity Impact</td><td>Availability Impact</td></tr>
<tr><td>Network</td><td>Low</td><td>None</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="6">CVSS Temporal Score - 8.3</td></tr>
<tr><td colspan="2">Exploitability</td><td colspan="2">Remediation Level</td><td colspan="2">Report Confidence</td></tr>
<tr><td colspan="2">Functional</td><td colspan="2">Official-Fix</td><td colspan="2">Confirmed</td></tr>
</table>

影響

この脆弱性の不正利用に成功すると、攻撃者が Cisco NAC Manager で任意のクエリを実行し、該当システムの制御権を取得する可能性があります。
攻撃に成功した場合、認証されていない攻撃者によって NAC Manager データベース内のユーザ名やパスワード ハッシュなどの情報がアクセス、作成、または変更される可能性があります。また、該当デバイスで任意のファイルやシステム ファイルが作成、変更、または削除されたり、機

密情報がコピーされたりする可能性もあります。

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。

この脆弱性は、NAC Manager バージョン 4.9.2、4.8.3.1 以降で修正されています。

Cisco NAC Manager は、次のリンクでダウンロードできます。

http://software.cisco.com/download/navigator.html?mdfid=279515766&i=rm/

回避策

このドキュメントに記載されている脆弱性に対する回避策はありません。

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 Nenad Stojanovski 氏によって発見され、ZDI から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-20130417-nac/

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-April-17	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。