NTTデータ・セキュリティ株式会社

Cacti の複数の脆弱性(CVE-2009-4032)に関する検証レポート

2009/11/30
NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

Cacti に複数の脆弱性が存在することが発見されました。
Cacti（カクタイ）とは、サーバ監視などに用いられる SNMP エージェントから、取得した値をグラフ化するフロントエンドプログラムです。

今回発見された複数の脆弱性は下記の通りです。

① クロスサイトスクリプティングの脆弱性
② OS コマンドインジェクションの脆弱性

今回、この Cacti の複数の脆弱性（CVE-2009-4032）の再現性について検証を行いました。

【影響を受けるとされているシステム】

Cacti 0.8.7e を含む、0.8.7e 以前のバージョン

【対策案】

① クロスサイトスクリプティングの脆弱性

修正プログラムがリリースされております。
十分な検証の後、運用に支障をきたさないことをご確認の上、修正プログラムの適用を行うことが推奨されます。
http://www.cacti.net/downloads/patches/0.8.7e/cross_site_fix.patch

② OS コマンドインジェクションの脆弱性

このレポート作成現在(2009 年 11 月 30 日)、OS コマンドインジェクションの脆弱性については、修正プログラムがリリースされておりません。
この脆弱性を利用するには、Cacti へのログインが必須条件となります。そのため、今一度、Cacti のログインアカウントに脆弱なパスワードが設定されていないか確認し、必要に応じ強固なパスワードへの変更を行っていただくことが推奨されます。

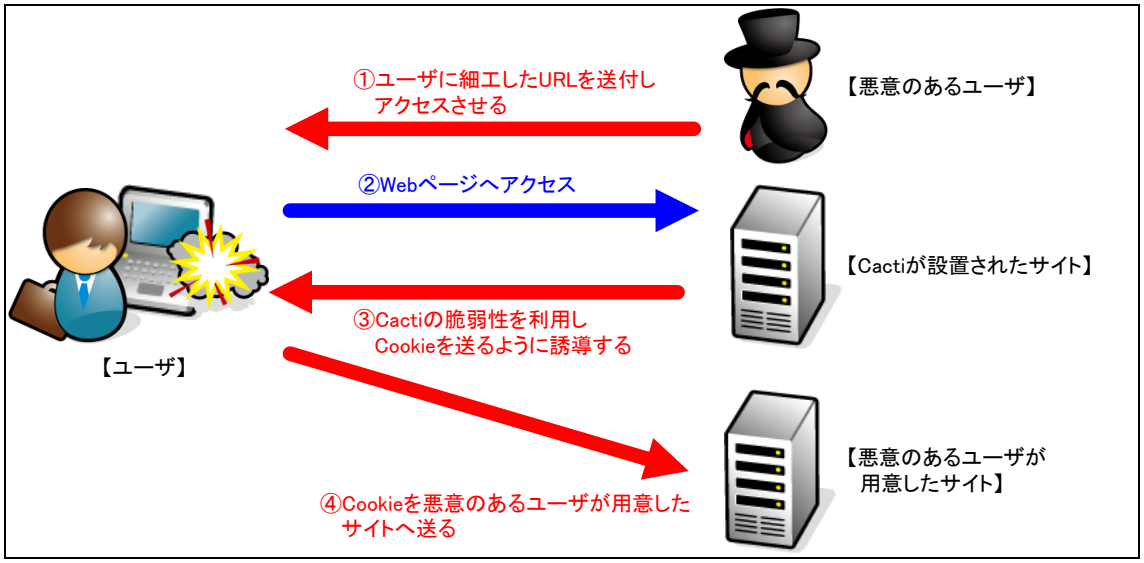
【参考サイト】

CVE-2009-4032
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4032

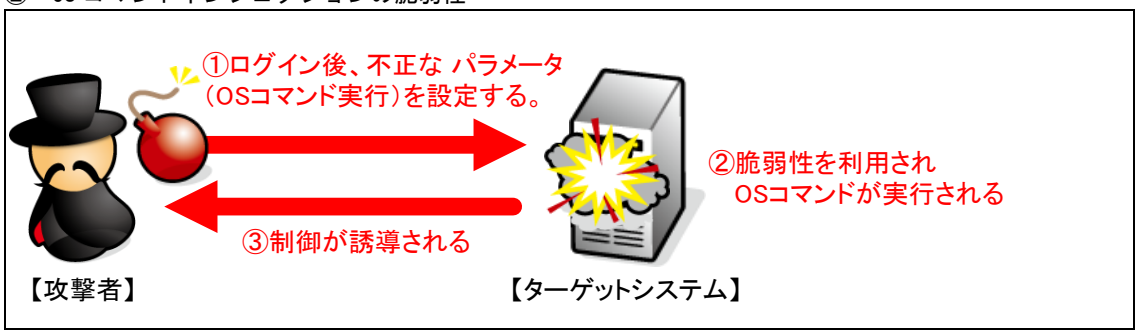
Copyright © 2009. NTT DATA SECURITY CORPORATION All right reserved.

【検証イメージ】

① クロスサイトスクリプティングの脆弱性



② OS コマンドインジェクションの脆弱性



【検証ターゲットシステム】

CentOS 5
Cacti 0.8.7e

【検証概要】

① クロスサイトスクリプティングの脆弱性

サイト利用者に、細工した URL にアクセスさせることで、脆弱性を含む Cacti が設置されたサイトの Cookie を取得します。
今回の検証に用いたスクリプトは、アラートのポップアップを表示させるものです。
※本脆弱性は、Cacti にログインできることが前提条件です。

② OS コマンドインジェクションの脆弱性

Cacti にログイン後、パラメータを設定することで、任意の OS コマンドを実行します。
実行させるコマンドは、ターゲットシステムの制御を別の誘導先コンピュータ（Windows XP）に移すというものです。
※本脆弱性は、Cacti にログインできることが前提条件です。

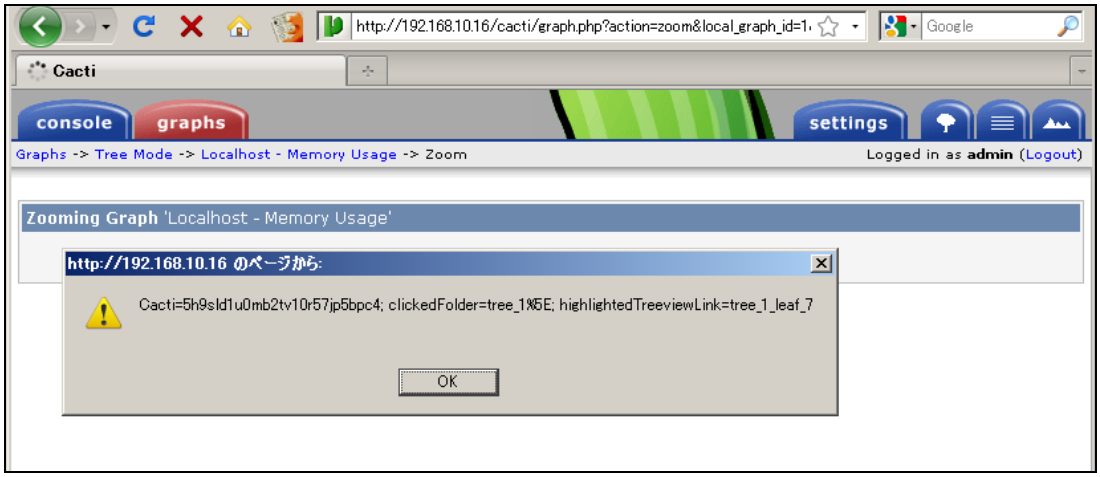
Copyright © 2009. NTT DATA SECURITY CORPORATION All right reserved.

【検証結果】

① クロスサイトスクリプティングの脆弱性

下図は、クロスサイトスクリプティングの攻撃を実行した後のターゲットシステムの画面です。
これにより、ターゲットシステムで任意のスクリプトが実行可能であると言えます。

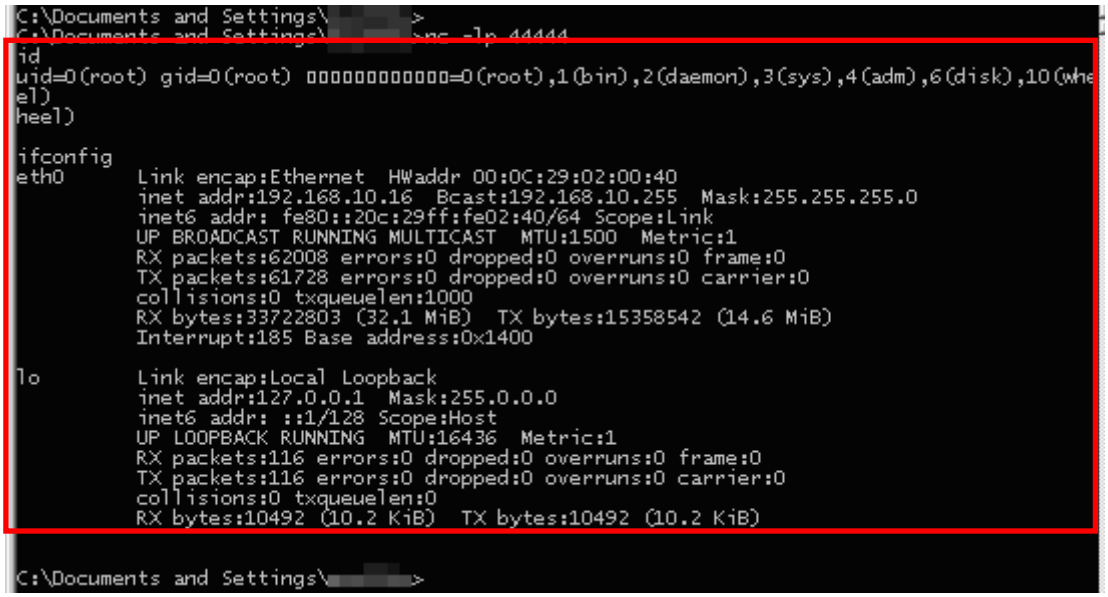
ターゲットシステムで任意のスクリプト実行に成功した画面



② OS コマンドインジェクションの脆弱性

下図は、OS コマンドインジェクションの攻撃を実行し、制御を別のコンピュータに誘導した画面です。
赤線で囲まれている部分が示すように、誘導先コンピュータ（Windows XP）のコマンドプロンプト上にターゲットシステム（CentOS 5）のコマンド実行結果が表示されています。
これにより、ターゲットシステムの制御の奪取に成功したと言えます。

ターゲットシステムで任意のコマンド実行に成功した画面



Copyright © 2009. NTT DATA SECURITY CORPORATION All right reserved.

NTTデータ・セキュリティ株式会社

＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ・セキュリティ株式会社
営業企画部
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/

Copyright © 2009. NTT DATA SECURITY CORPORATION All right reserved.