NTTデータ・セキュリティ株式会社

Cacti の設定項目における OS コマンドインジェクションの脆弱性に関する検証レポート

2010/4/26
NTT データ・セキュリティ株式会社
辻 伸弘

【概要】

Cacti に OS コマンドインジェクション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、この Cacti の OS コマンドインジェクションの脆弱性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 以前のバージョン

【対策案】

このレポート作成現在（2010 年 4 月 26 日）、この脆弱性に関する修正プログラムはリリースされていません。
また、この脆弱性を利用するには、「Console Access」と「Update Data Sources」または「Update Graph Templates」の権限を有するユーザで Cacti へのログインが可能であることが必須条件となります。
そのため、今一度、Cacti のアカウントに脆弱なパスワードが設定されていないこと、アカウントへ付与する権限が適切であることを確認してください。さらに、必要に応じ強固なパスワード設定、適切な権限付与設定を実施していただくことが推奨されます。
また、Cacti に接続可能なアクセス元の制限を実施していただくことも併せて推奨されます。

【検証イメージ】

【検証ターゲットシステム】

CentOS 5
Cacti 0.8.7e

【検証概要】

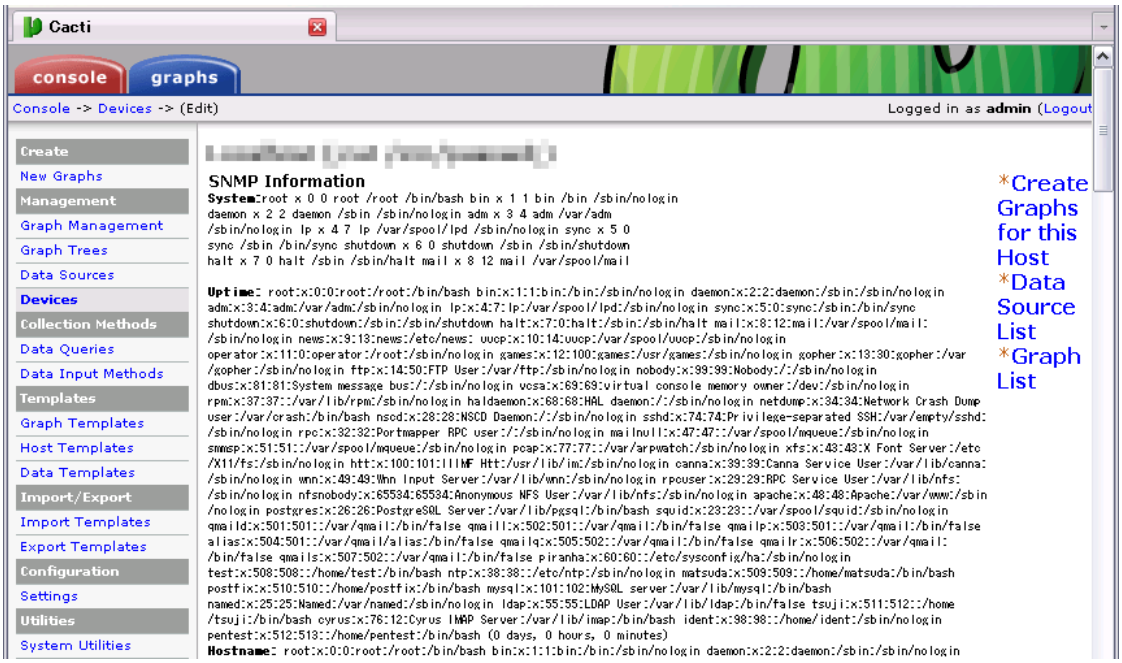
Cacti にログイン後、パラメータを設定することで、任意の OS コマンドを実行します。
実行させるコマンドは、「/etc/passwd」ファイルの表示です。
※本脆弱性は、Cacti にログインできることが前提条件です。

NTTデータ・セキュリティ株式会社

【検証結果】

下図は、パラメータを不正に操作し「cat」コマンドを用いて「/etc/passwd」ファイルを表示させるコマンドを挿入し、実行に成功した画面です。画面上には、Cacti の設定内容ではなく、「/etc/passwd」の内容が表示されていることから OS コマンドインジェクションに成功したと言えます。

センシティブ情報「/etc/passwd」の窃取



＊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
企画部　広報グループ
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/