NTTデータ・セキュリティ株式会社

Nagios の statuswml.cgi の脆弱性(CVE-2009-2288)に関する検証レポート

2009/7/6
診断ビジネス部
辻 伸弘
松田 和之

【概要】

Nagios の statuswml.cgi ファイルにコマンドインジェクションを受ける脆弱性が存在することが発見されました。
この脆弱性により、リモートから Web サービスの実行権限で任意のコマンドが実行可能となります。
Nagios とは、ブラウザからホストの稼動状態を監視可能にするプログラムです。
コマンドインジェクションとは、ホストへのリクエスト内に OS コマンドを不正に埋め込み（インジェクション）、ホスト上で OS コマンドを実行させる攻撃手法です。

想定される被害としては、悪意のあるユーザにより、Web サービスの実行権限での情報取得、改ざん、または、悪意あるプログラムをシステム内にインストールされることが考えられます。

今回、こ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】

Nagios 3.1.1 より前のバージョン

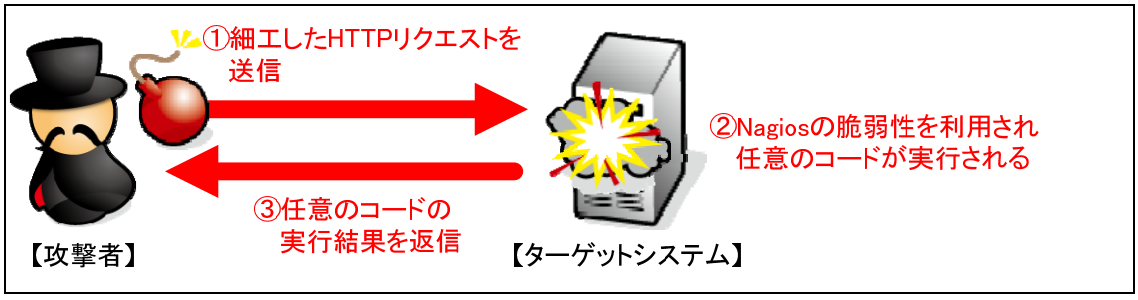
【対策案】

最新バージョン（Nagios 3.1.2）へアップデートすることが推奨されます。
http://www.nagios.org/download/

【参考サイト】

CVE-2009-2288
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2288
Nagios 3 Version History
http://www.nagios.org/development/history/core-3x/

【検証イメージ】



【検証ターゲットシステム】

Nagios 3.0.6

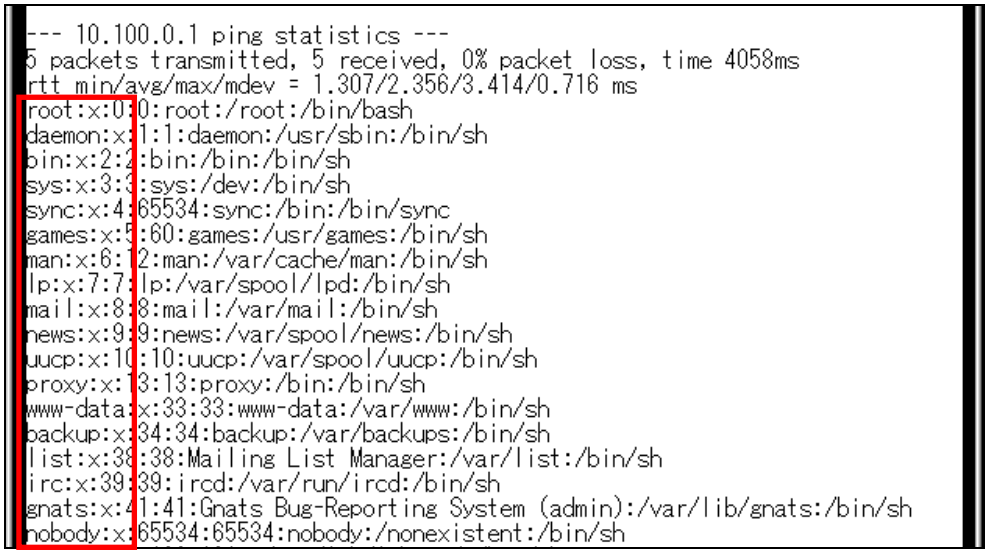
【検証概要】

ターゲットシステムに、細工した HTTP リクエストを送信することで、任意のコマンドを実行します。

【検証結果】

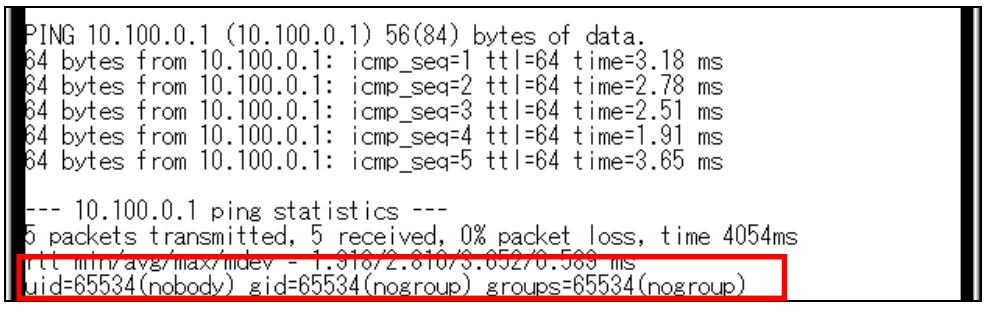
下図は、Nagios の statuswml.cgi の脆弱性を利用し、ターゲットシステムのユーザ情報が格納されている「/etc/passwd」ファイルを、ブラウザから読み出した画面です。
赤枠（赤枠内の「：」（コロン）より前の部分）で示すとおり、ターゲットシステムに存在するユーザの一覧の取得に成功したと判断できます。これにより、悪意のあるユーザに、SSH 等から当該ユーザに対するオンラインクラックを行われ、システムへの更なる制御の奪取を許す危険性があります。
また、プログラムのソースコードも閲覧可能であるため、ソースコード内にデータベースへのログインパスワードが記述されている場合、パスワードを取得され、なりすましに利用される危険性があります。

ターゲットシステムの/etc/passwd を読み出した画面



下図は、ターゲットシステム上で id コマンドを実行した画面です。このことから、当脆弱性を利用することで、Web サービスの実行権限でのコマンド実行が可能であると判断できます。つまり、Web サービスが管理者権限で稼動している場合、ターゲットシステムに存在する暗号化されたパスワードも読み出すことが可能となります。

ターゲットシステムで id コマンドを実行した画面



【対策案】

最新バージョン（Nagios 3.1.2）へアップデートすることが推奨されます。

http://www.nagios.org/download/

【参考サイト】

CVE-2009-2288

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2288

Nagios 3 Version History

http://www.nagios.org/development/history/core-3x/

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/