NTT DATA
NTTデータ 先端技術株式会社

nginx のチャンク・エンコーディングされたリクエストを処理する際の脆弱性により、任意のコードが実行される脆弱性(CVE-2013-2028)に関する検証レポート

2013/6/6
NTT データ先端技術株式会社
辻　伸弘
泉田　幸宏
鈴木　宏信

【概要】

nginx に、リモートより任意のコードを実行される脆弱性が発見されました。
この脆弱性は、チャンク・エンコーディングされたリクエストを処理するプロセスにて、細工されたリクエストが送信された場合にオーバーフローが発生する欠陥に起因します。この脆弱性を悪用して、攻撃者はターゲットホスト上にて、nginx の worker プロセスの動作権限で任意のコードの実行が可能です。

今回、このバッファオーバーフローにより任意のコードを実行される脆弱性（CVE-2013-2028）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】

影響を受ける可能性が報告されているのは次の通りです。
- nginx 1.3.9
- nginx 1.4.0

※nginx は、ブラウザからアプライアンス製品の設定変更・確認などの管理方法を提供するための Web サーバやリバースプロキシ、ロードバランサ機能の提供に使用されている場合があります。
そのため、ご利用されているアプライアンス製品にて nginx が使われているかの仕様をマニュアルなどで確認していただくか、ベンダにお問い合わせいただき確認していただくことを推奨いたします。

【対策案】

この脆弱性が修正された最新版 nginx 1.4.1 または nginx1.5.0 にアップデートしていただく事を推奨いたしますが、アップデートが実施できない場合は nginx の公式サイトにて公開されている修正方法をご確認ください。

nginx ダウンロードサイト
http://nginx.org/en/download.html

修正方法
http://mailman.nginx.org/pipermail/nginx-announce/2013/000112.html

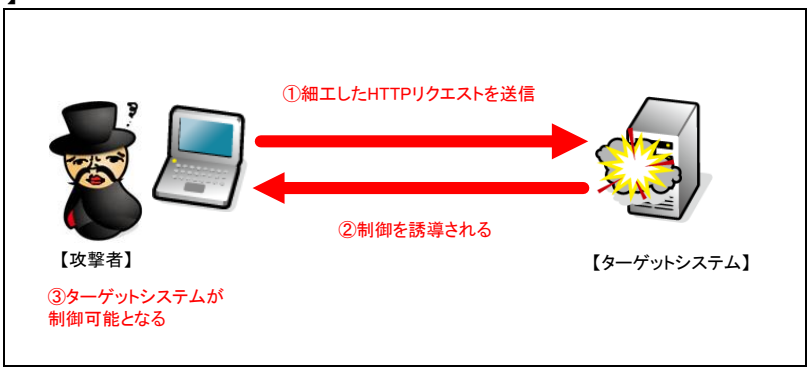
【参考サイト】

CVE-2013-2028
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2028

nginx security advisories
http://nginx.org/en/security_advisories.html

Copyright © 2013. NTT DATA INTELLILINK CORPORATION All right reserved.

【検証イメージ】



【検証ターゲットシステム】
Ubuntu 13.04 上の nginx 1.4.0

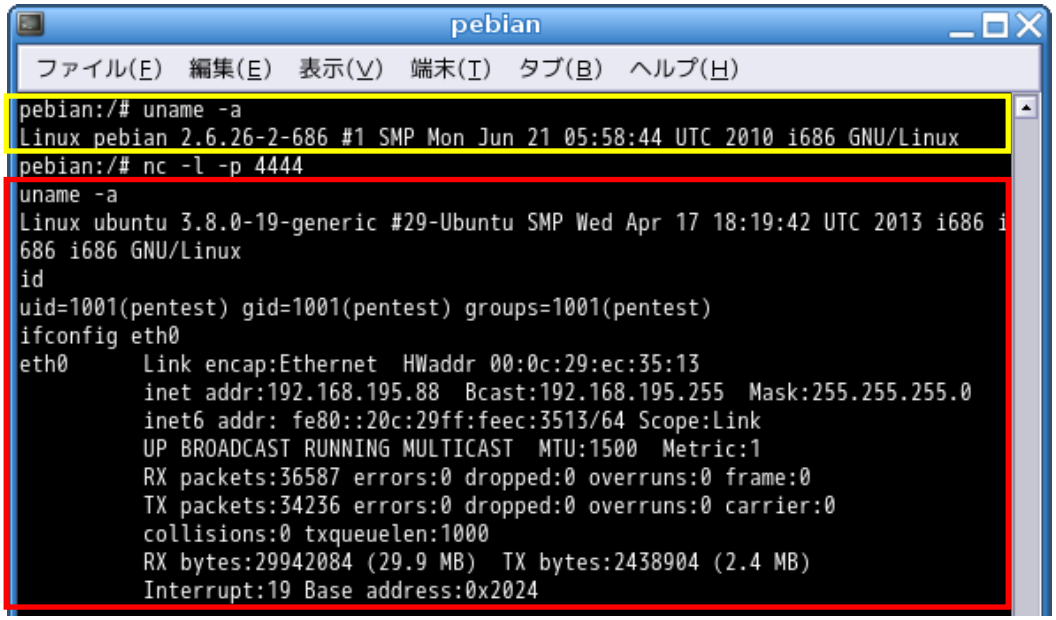
【検証概要】
ターゲットシステムに、細工した HTTP リクエストを送信し、任意のコードを実行させます。
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムを操作可能となります。
＊誘導先のシステムは Debian です。

Copyright © 2013. NTT DATA INTELLILINK CORPORATION All right reserved.

【検証結果】

下図は、攻撃後の誘導先のコンピュータ（Debian）の画面です。黄線で囲まれている部分は、誘導先のコンピュータのホスト情報です。一方、赤線で囲まれている部分は、ターゲットシステム（Ubuntu13.04）において、コマンドを実行した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の制御の奪取に成功した画面



＊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 データ先端技術株式会社
セキュリティ事業部
TEL:03-5859-5422
http://security.intellilink.co.jp

Copyright © 2013. NTT DATA INTELLILINK CORPORATION All right reserved.