NTTデータ先端技術株式会社

vsftpd 2.3.4 に含まれたバックドアに関する検証レポート

2011/07/06
NTT データ先端技術株式会社
辻　伸弘
小田切　秀暁

【概要】

vsftpd のバージョン 2.3.4 のソースファイル「vsftpd-2.3.4.tar.gz」にリモートから任意のコードの実行を可能にするバックドアコードが含まれていました。

バックドアコードを含んだ状態で vsftpd をインストールおよび起動すると、特定の文字列「:)」を含むユーザー名で FTP 接続した際にバックドアポートである TCP6200 番がオープンします。バックドアポートにリモートから接続すると任意のコマンドが実行可能となります。

今回、このバックドア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アプリケーション】

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。

・vsftpd 2.3.4

※2011 年 7 月 6 日現在、上記バージョンのソースコードはバックドアの影響を受けないソースコードに修正されています。
ソースコード入手先：
https://security.appspot.com/downloads/vsftpd-2.3.4.tar.gz

【対策案】

vsftpd 2.3.4 をインストールする場合 GPG 署名の確認を実施いただくことを推奨いたします。
また、バックドアコードを含んだソースファイル「vsftpd-2.3.4.tar.gz」のチェックサム（sha256sum）および、PGP 署名が公開されています。下記に該当しないかどうか確認いただくことを推奨いたします。

```
sha256sum:
2a4bb16562e0d594c37b4dd3b426cb012aa8457151d4718a5abd226cef9be3a5
vsftpd-2.3.4.tar.gz

gpg:
Signature made Tue 15 Feb 2011 02:38:11 PM PST using DSA key ID 3C0E751C
```

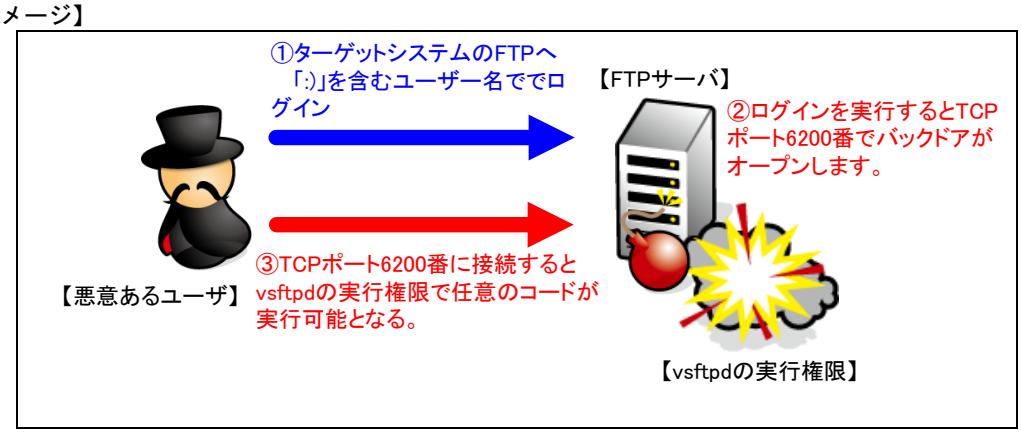
現在動作している vsftpd にバックドアコードが含まれているか、実際に FTP 接続を実施することも対策となります。本レポートを参考に管理サイトに接続し TCP ポート 6200 番がオープンにならないことを確認ください。

さらに、外部から FTP サーバの不要なポートに接続できないようにアクセス制御を実施いただくことを推奨いたします。

【参考サイト】

Alert: vsftpd download backdoored / SECURITY HACKING EVERYTHING, BY CHRIS EVANS / SCARYBEASTS
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

【検証イメージ】

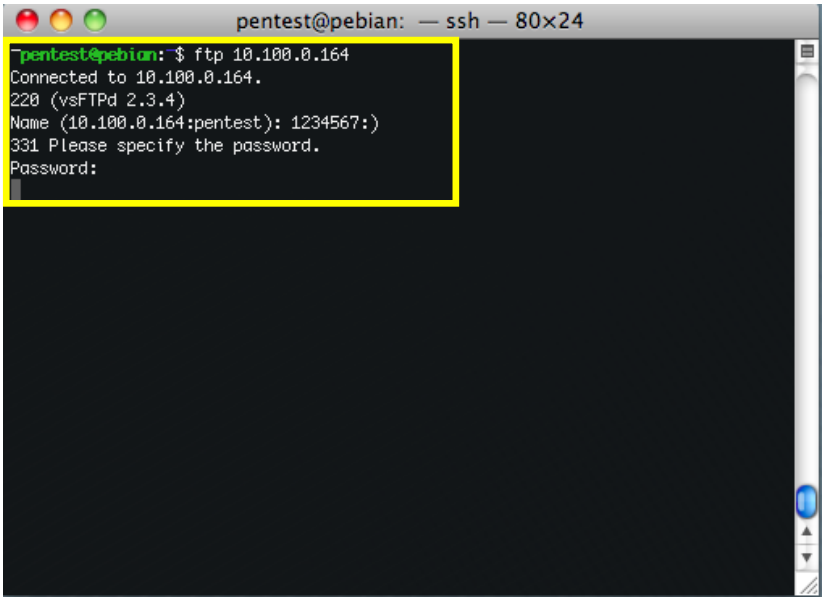


【検証ターゲットシステム】
Debian 6.0 およびバックドアコードを含んだ vsftpd 2.3.4

【検証概要】
ターゲットシステム上でバックドアコードを含んだ vsftpd を起動します。そして、ターゲットシステムに FTP 接続を実施しオープンしたバックドアポートである TCP ポート 6200 番に接続します。

【検証結果】
黄枠にあるとおり事前に FTP サーバに認証を行います。認証を実行すると 6200 番ポートがオープンします。その後、赤枠にあるとおり TCP6200 番に接続するとターゲットシステム（Debian 6.0）上のシェルが表示されます。
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。

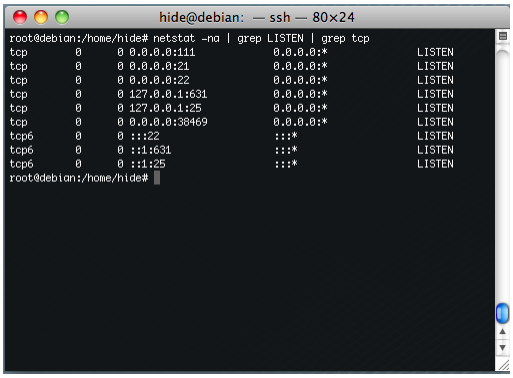
ターゲットシステムに FTP 接続した画面



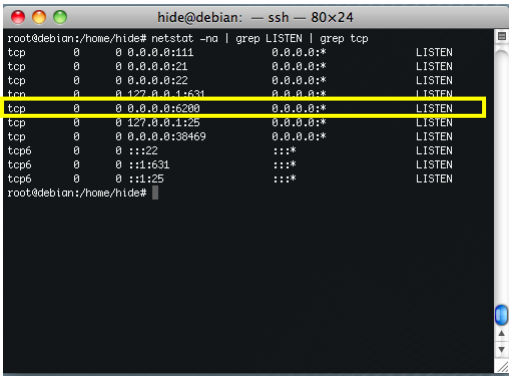
NTTデータ先端技術株式会社

TCP6200 番がオープンした状態

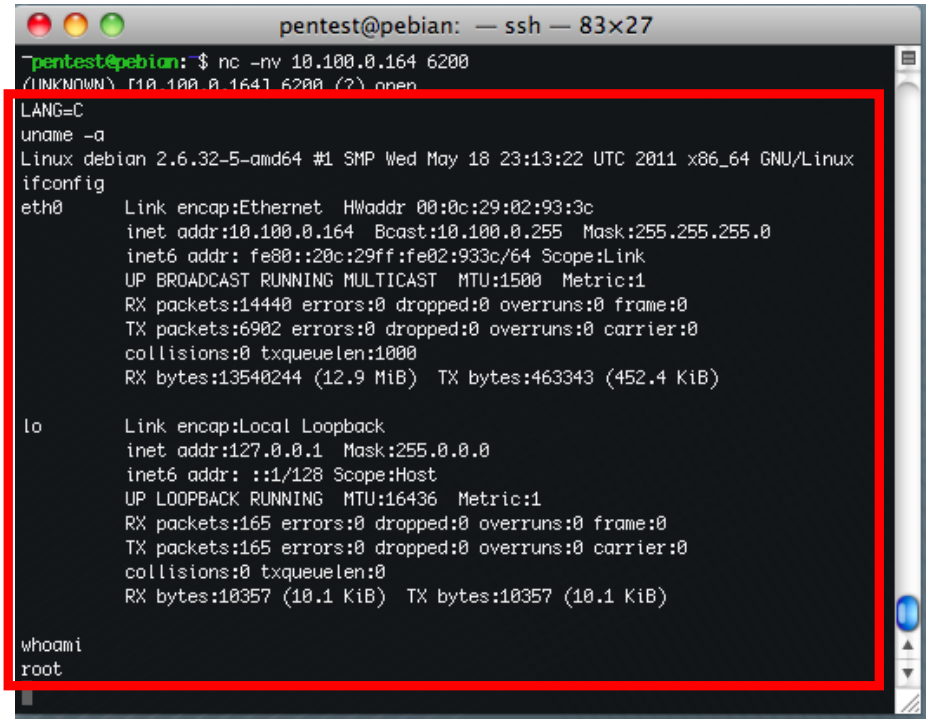
認証前



認証後



バックドアポート（TCP6200 番）に接続し
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　営業担当　営業企画グループ
TEL:03-5425-1954
http://security.intellilink.co.jp/