SoftBank Technology

ソフトバンク・テクノロジー株式会社

脆弱性調査レポート

ProFTPD の脆弱性により、リモートから任意のファイルをコピー可能な脆弱性（CVE-2015-3306）に関する調査レポート

【概要】

ProFTPD のモジュールである mod_copy が一部の SITE コマンドを処理する際に、リモートから任意のファイルをコピー可能な脆弱性（CVE-2015-3306）が発見されました。この脆弱性は、細工された FTP コマンドをターゲット上の ProFTPD に送信することにより、ターゲット内の任意のファイルをターゲット上にコピー可能です。
この脆弱性を利用した攻撃が成立した場合、リモートから ProFTPD の実行権限を奪取される危険性があります。

ただし、本脆弱性を攻撃に利用し、外部から実害（本レポートでは、リモートから任意のコードを実行することを指します）を与えるためには、ProFTPD が生成するログに対して第三者権限に読み取り権限が与えられていること、かつ、Web サーバーが稼動しており、その Web サーバーの公開ディレクトリに ProFTPD の動作権限に書き込み権限が与えられていることが必要条件です。

本レポート作成（2015 年 4 月 30 日）時点において、ソース版についてはベンダーより脆弱性を修正したバージョンがリリースされております（2015 年 4 月 7 日にリリース）。しかしながら、攻撃を成立させるためのコードが容易に入手可能であり、かつ脆弱性に対する攻撃が容易であることから、今回、この脆弱性（CVE-2015-3306）の再現性について検証を行いました。

【影響を受けると報告があるシステム】

- ProFTPD 1.3.5 系のソース版
- Debian （wheezy）の ProFTPD 1.3.4a-5+deb7u2 および、1.3.4a-5+deb7u1
- Debian （jessie）の ProFTPD 1.3.5-1.1
- Fedora epel7

【対策案】

ProFTPD のソース版を利用している場合、脆弱性を修正したバージョンがベンダーの github で管理されています。ただし開発版の位置づけですので、導入される前に十分な検証を行っていただくことを推奨します。
OS のパッケージ版を利用している場合、OS ベンダーに対してこの脆弱性について問い合わせていただくことを推奨します。

なお、以下のコマンドを実行することにより、この脆弱性の影響を受けるか否かを確認可能です。

```
telnet <IP アドレス> <ProFTPD が動作するポート番号>
site cpfr （任意のファイル）
site cpto （ProFTPD の実行権限で書き込めるパス（例えば/tmp）＋任意のファイル名）


【コマンド例】
telnet 10.0.0.128 21
220 ProFTPD 1.3.4a Server (Deb7-proftpd) [10.0.0.128]
site cpfr /etc/passwd
350 ファイルまたはディレクトリが存在します。他の名前にしてください。
site cpto /tmp/test.txt
250 Copy successful
quit
221 さようなら.
Connection closed by foreign host.

ls /tmp
test.txt
```

コマンド実行後、site cpto コマンドにより指定したファイルが作成されていることが確認できた場合、脆弱性の影響を受けます。上記のように、認証無しで外部からは閲覧できないディレクトリに対しても、ProFTPD の実行権限で参照可能なファイルを、ProFTPD の実行権限で書き込み可能となります。脆弱性の影響を受ける場合、任意のファイルをコピーすることが可能です。

【参考サイト】

- CVE-2015-3306

- bug 4169 – Unauthenticated copying of files via SITE CPFR/CPTO allowed by mod_copy

【検証概要】

ProFTPD が動作するターゲットシステムに対して細工した FTP コマンドを送信することにより、ターゲットシステムで動作している Web サーバーの公開ディレクトリ上に、ターゲット内のファイルをコピーし、そのファイルにブラウザでアクセスすることにより、最終的に任意のコードの実行結果をブラウザに出力させます。
なお今回の検証のために、Web サーバーの公開ディレクトリと ProFTPD が生成するログのパーミッションに第三者権限に対して書き込みを与えております。

【検証ターゲットシステム】

Debian 上で動作する ProFTPD パッケージ 1.3.4a-5+deb7u2

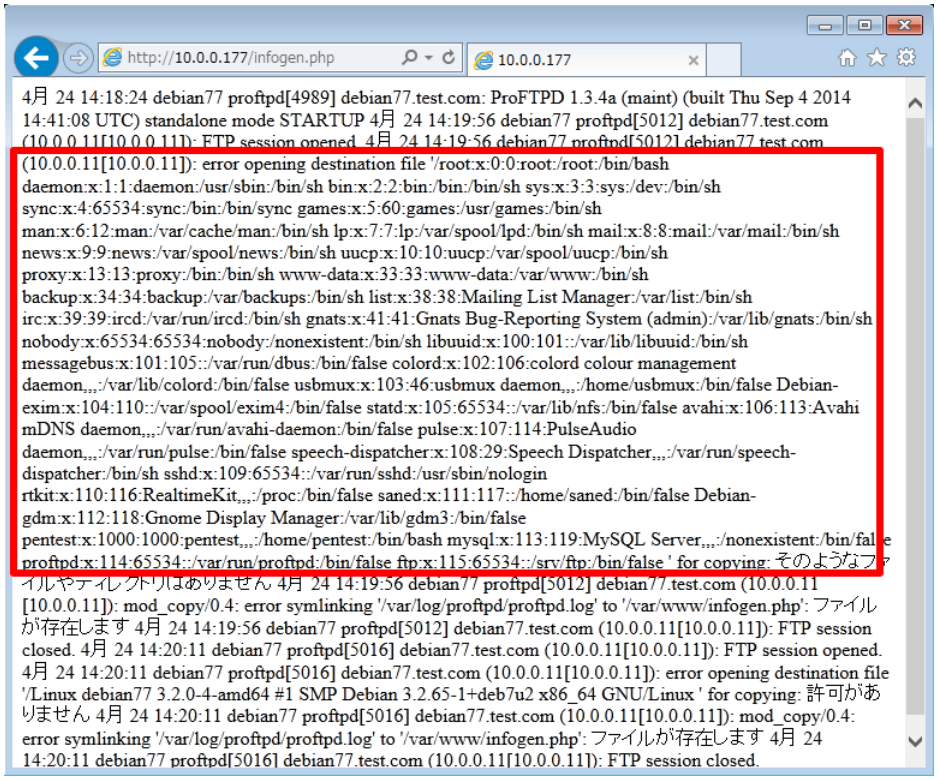
（および、PHP が動作可能な Web サーバー）

【検証イメージ】

【検証結果】

下図は、ターゲットシステム（Debian）で動作する Web サーバーに対して、ブラウザでアクセスした際の画面です。赤線で囲まれている部分は、ターゲットシステムの/etc/passwd の内容を表示する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、ProFTPD の脆弱性を利用して、ターゲットシステムで任意のコマンドを実行するためのファイルを作成し、Web サーバーの公開ディレクトリにコピーして参照することに成功しました。



その他、この脆弱性を利用して内部の特定の情報を外部から参照可能となる構成例を以下に記述します。

構成	パターン	結果
ProFTPD のみ	Anonymous ログインが有効であり、かつ ProFTPD の実行権限と Anonymous ユーザーの権限が同じである場合	FTP の Anonymous ディレクトリに任意のファイルをコピーでき、Anonymous ユーザーがそのファイルを参照可能
ProFTPD ＋Web サーバー ＋PHP	Web サーバーの公開ディレクトリのパーミッションに、第三者権限に対して書き込み権限が与えられている場合	Web サーバーの第三者権限に書き込みの許可を与えているディレクトリに、任意のファイルをコピーでき、Web ブラウザよりそのファイルを参照可能
	上記に加えて、ProFTPD のログファイルに第三者権限に対して読み取り権限が与えられている場合 ※今回の検証のパターンです	Web サーバーの第三者権限に書き込みの許可を与えているディレクトリに、任意のコマンドの出力結果をファイルとして生成でき、Web ブラウザよりそのファイルを参照可能

【更新履歴】

2015 年 4 月 30 日 ： 初版公開

ソフトバンク・テクノロジー株式会社
〒160-0022 東京都新宿区新宿６丁目 27 番地 30 号
新宿イーストサイドスクエア 17 階
受付時間：平日 10:00～17:00

電話 03-6892-3154
メール sbt-ipsol@tech.softbank.co.jp
URL https://www.softbanktech.jp/