Monthly Research

WordPress の脆弱性を狙った Web 改ざん攻撃

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.02

はじめに

- 近年の Web 改ざんは、マルウェア感染を目的としたものが主流であったが、ここ数年では、主義主張の顕示を目的とする改ざんも、再び目立つようになっている。

- その中でも、明確なターゲットを定めず多く普及している CMS やそのプラグインの脆弱性を突いて、無差別に大量のサイトを改ざんする攻撃が増加している
  - 2014年7月には WordPress から簡単にメールマガジンを配信できる人気プラグイン「MailPoet Newsletters」の脆弱性を利用して、50,000件ものWeb サイトが改ざんされた

- 今回の Monthly Research では特に WordPress を標的とした攻撃の内、2015年に入って急増した攻撃手法とその対策について解説を行う

被害状況

- 全体での被害統計は測定が不可能であるため、この攻撃手法による改ざん報告が特に多かった「Index Php」と名乗る人物が「www.zone-h.org」に投稿した情報の統計を以下に示す

- 2015年4月6日から 7日の24時間で、日本のドメインを含む少なくとも 1,200 件以上の WordPress を利用するサイトが改ざん被害を受けた

- この攻撃は 2015年3月末頃から発生しており、これまでで少なくとも 18,000 件以上のサイトが被害にあっている。この内の 125 件は日本のドメインである。

- この攻撃では、直接ファイルを改ざんするのではなく、特定の URI にアクセスした際に、攻撃者が注入した内容のページが表示されるタイプであった

攻撃分析

- 攻撃成功を示す URL は共通して以下の様なものであった
  「http://target.com/wp-admin/admin-ajax.php?action=revslider_ajax_action&client_action=get_captions_css」

- 「**wp-admin**」が含まれていることから、**WordPress**を標的とした攻撃だということが推測される
- WordPress 上での Ajax 通信をサポートする「admin-ajax.php」に対して「action=**revslider_ajax_action**」という内容の引数が渡されている事から、国内でも多く利用されているプラグイン「**Slider Revolution**」へのリクエストであることが推測される
- 更に「client_action=**get_captions_css**」が引数として指定されていることが分かる

攻撃分析

- 前スライドの分析結果と攻撃の発生時期(2015年3月末)、早い時期からこの攻撃手法を使用している人物、チームなどを調査した結果、実際に使用されていると思われる、大量改ざん用に作成されたスクリプトの存在を把握した。

- 他にも多数の PoC が Pastebin などで公開されている

攻撃分析

- 公開された PoC を見ると以下の様な POST データを「admin-ajax.php」に対して送信していることが分かる

```
$post = array?>
(
"action" => "revslider_ajax_action",
"client_action" => "update_captions_css",
"data" => "<marquee>Malicious Code Here</marquee>"
);
```

攻撃分析

- ここで Slider Revolution 側のソースコードを見てみると「revslider_admin.php」に以下の様な記述がある

```
232.    $action = self::getPostGetVar("client_action");
233.    $data = self::getPostGetVar("data");
...
301.    case "get_captions_css":
302.        $contentCSS = $operations->getCaptionsContent();
303.        self::ajaxResponseData($contentCSS);
...
305.    case "update_captions_css":
306.        $arrCaptions = $operations->updateCaptionsContentData($data);
307.        self::ajaxResponseSuccess("CSS file saved
            succesfully!",array("arrCaptions"=>$arrCaptions));
```

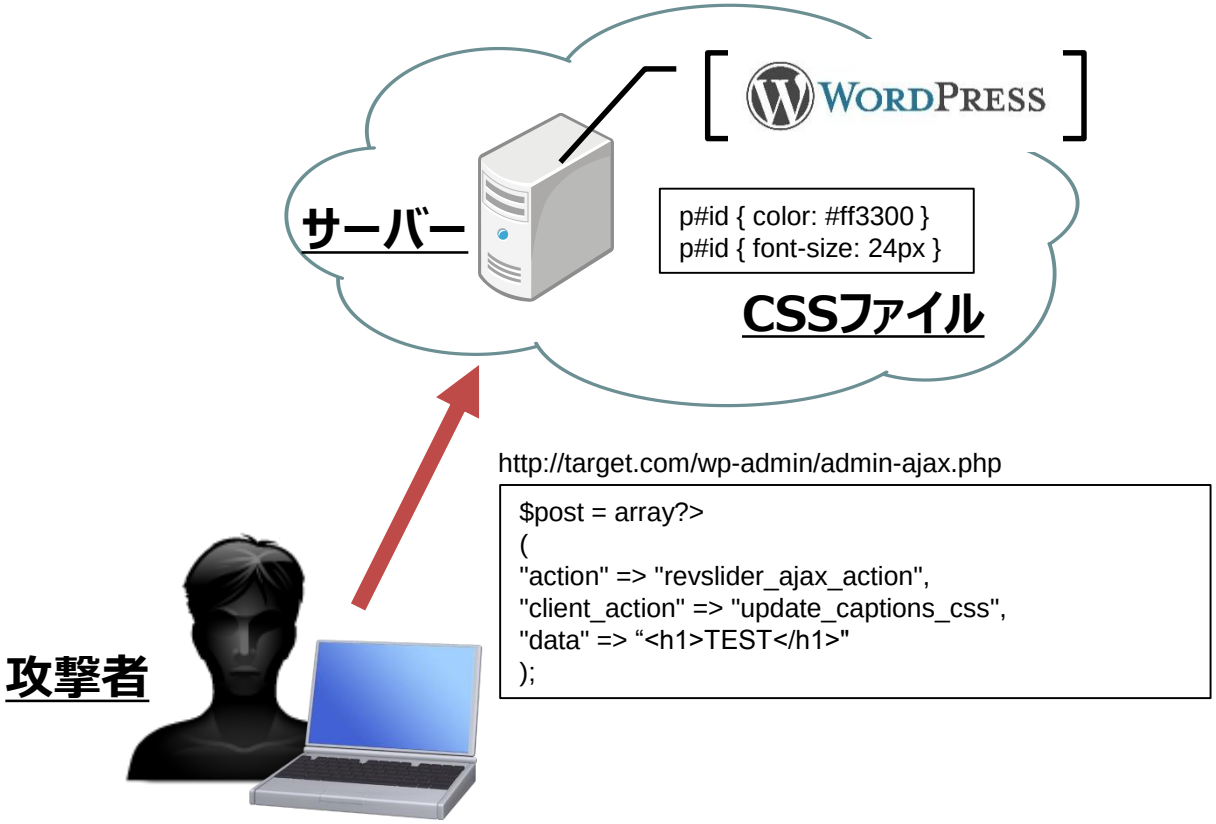
攻撃分析

- 前スライドの記述から次のようなことが分かる
  - POST されてきた「client_action」の値から「get_captions_css」もしくは「update_captions_css」を呼び出す
  - 「**get_captions_css**」を指定した場合は、予め用意された CSS ファイルを取得して Ajax 通信のレスポンスとして返す
  - 「**update_captions_css**」を指定した場合は、予め用意されている CSS ファイルに POST されてきた「data」の値を上書きする

- これらの事から攻撃者はまず、「update_captions_css」を不正に呼び出し、指定した任意の文字列、もしくはコードを後に呼び出される CSS ファイルに保存し、閲覧者に対して「get_captions_css」のレスポンスを示すことで改ざんを行っていたという事が分かる

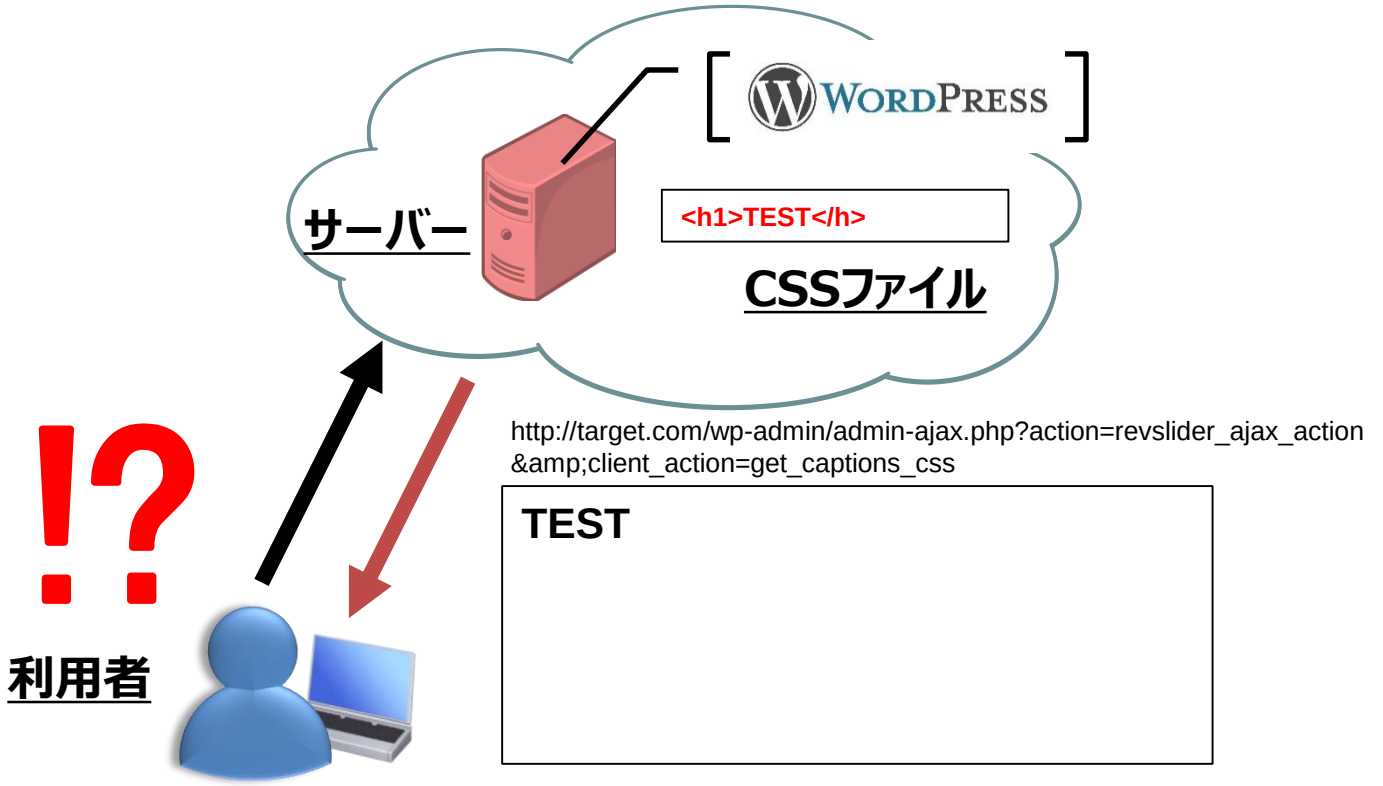
攻撃の流れ

「/wp-admin/admin-ajax.php」に対して不正な POST リクエストを送ることによって、サーバー内の CSS ファイルを上書きする



攻撃の流れ

「get_captions_css」を呼び出すように細工された URL にアクセスすると、攻撃者が上書きした内容の CSS がレスポンスとして返ってくる



脅威分析

- 我々が入手したスクリプトでは Google 検索における検索構文を悪用することで、Google にインデックスされている脆弱な Web サイトやサーバーを大量に探しだすことができる、Google Dork と呼ばれる手法と組み合わせることで、世界中のサーバーに対して攻撃を行う方法が取られていた
  - Google Hacking Database
  - http://www.exploit-db.com/google-dorks/

脅威分析

- 以上の攻撃分析から、次のような脅威が考えられる
  - 不正な JavaScript を注入することで、Cookie 情報などを窃取される
  - DDoS 攻撃などを JavaScript ベースで行う攻撃の踏み台にされる
  - 同一生成元ポリシーの影響を回避した攻撃に発展される
  - マルウェア感染の踏み台として利用される
- これらの内、DDoS 攻撃への踏み台については、既にスクリプトが公開されている。

対策方法

- 有効な対策として以下が挙げられる
  - 「Slider Revolution」を脆弱性が修正されたバージョン(4.6.5)にアップデートする
  - 「.htaccess」などの設定で「/wp-admin/」や「/admin/」へのアクセスに制限をかける
  - クライアントアクション「update_captions_css」を無効にする
  - プラグインやテーマの自動更新機能を ON に設定し、使用していないプラグイン等は削除する
- プラグイン側のアップデートでの対策も、もちろん有効ではあるが、別のプラグインや WordPress 本体にも多く脆弱性が報告されているため、外部からの操作を受け付ける類の URI などにはアクセス制限をかけるなどの根本的な対策が重要になると考える
- また、そのような URI を「robots.txt」に追加することで前述の Google Dork での検索結果に表示されなくなる

まとめ

- 様々な目的から大量の Web サイトを無差別に改ざんする攻撃が増加している
  - その内、多く用いられる手法が WordPress などの、広く普及しているプロダクトの脆弱性、もしくはそれらの外部プラグインに存在する脆弱性を狙った攻撃である
- 今回は今年に入って、約 18,000 以上の Web サイトが被害にあった、「Slider Revolution」に関する脆弱性攻撃についての PoC を素に分析を行った
  - 従来の SQL インジェクションなどの脆弱性と大きく異なる点として、想定された機能が悪用されたという点が挙げられる
  - 本脆弱性を利用することで、安全とされている URL からマルウェアに感染させられる可能性も想定できる
- このような CMS 関連のプロダクトに関する攻撃の多くは管理者が利用することを前提とされた領域に多く見られる
  - そのため、「.htaccess」などの設定で「/wp-admin/」や「/admin/」へのアクセスに制限をかけることが有効な対策だといえる

参考情報

- 50,000 sites hacked through WordPress plug-in vulnerability
  http://www.pcworld.com/article/2458080/thousands-of-sites-compromised-through-wordpress-plugin-vulnerability.html
- Index Php | Zone-H.org
  http://www.zone-h.org/archive/notifier=Index%20Php
- Wordpress Plugin Revolution Slider - Unrestricted File Upload
  http://www.exploit4arab.net/exploits/1416

Contact Information

E-Mail ：research—feedback@ffri.jp
Twitter：@FFRI_Research