WordPress 插件Events Calendar 5.16.2 信息泄露漏洞(CVE-2021-24146)

事件背景

1. 研究背景：天眼日志分析
2. 事件名称：HTTP_漏洞利用_信息泄露_WordPress插件Modern_Events_Calendar_Lite
3. 修改字段：match
4. 数据来源：天眼日志对比
5. 研究深度：源码分析
6. 分析人员：周山
7. 分析时间：2023.6.19

漏洞说明

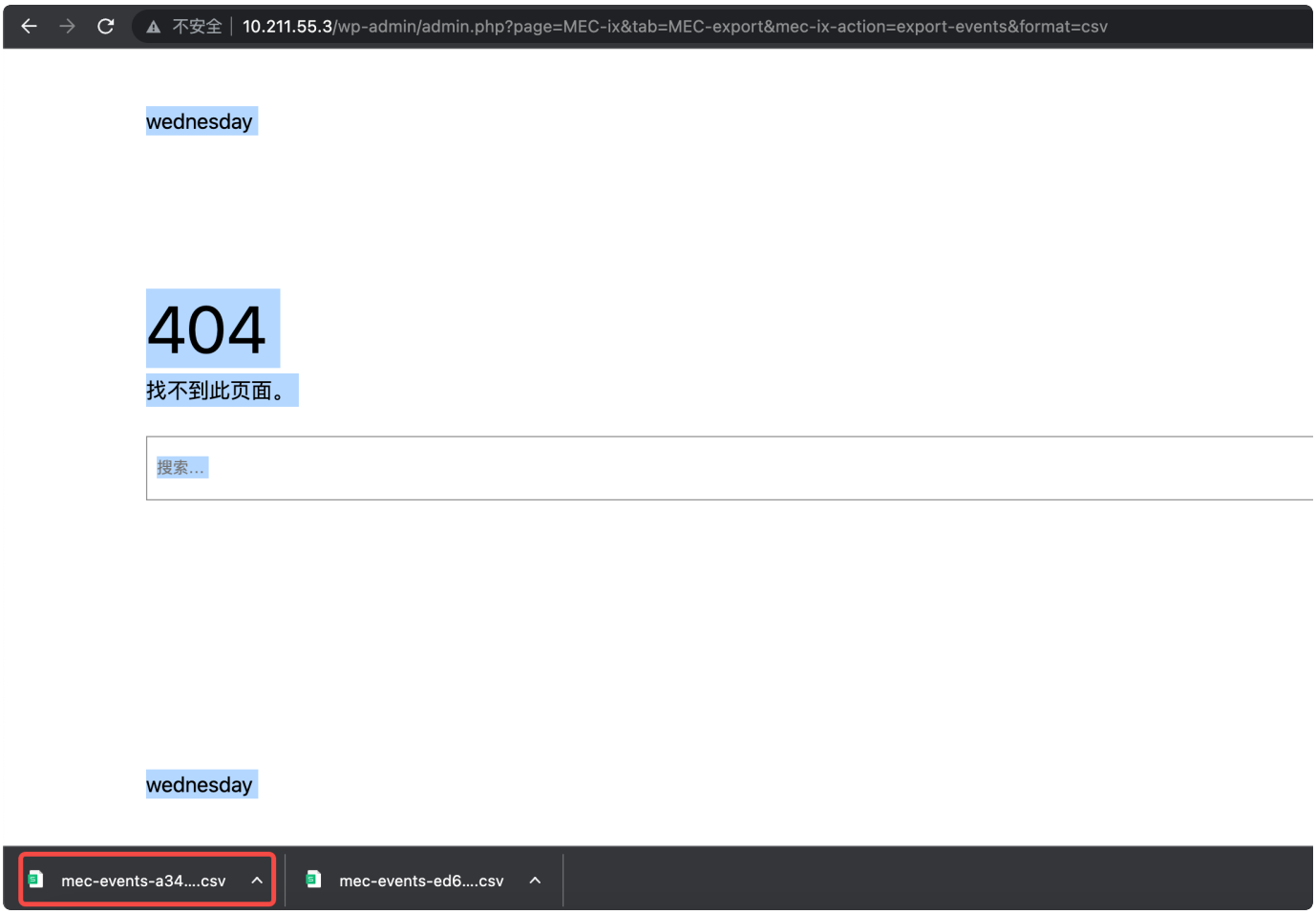
1. 漏洞原理：Modern Events Calendar Lite WordPress插件缺乏授权检查，5.16.5之前的版本没有正确限制对导出文件的访问，允许未经认证的用户导出CSV或XML格式的所有事件数据。
2. 组件描述：　Modern Events Calendar Lite是一款功能强大的WordPress插件，用于创建和管理活动日历。提供直观界面，支持添加、编辑和展示事件，包括时间、地点、票务等详细信息。可自定义多种日历视图，支持票务销售和数据导入导出。是一个灵活、易用的解决方案，适用于各类网站，提升活动管理和展示效果。
3. 影响版本：< Modern Events Calendar Lite v5.16.5

漏洞复现

poc

```
LaTeX  复制代码
```

```
GET /wp-admin/admin.php?page=MEC-ix&tab=MEC-export&mec-ix-action=export-events&format=csv HTTP/1.1
Host: 10.211.55.3
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: CookieLanguageName=ZH-CN; USER_NAME_COOKIE=admin; SID_1=6c0c974b; UI_COOKIE=0; hideTopbar=1; stylesheet=ayti; wp_lang=zh_CN; wordpress_test_cookie=WP+Cookie+check
Connection: close
```



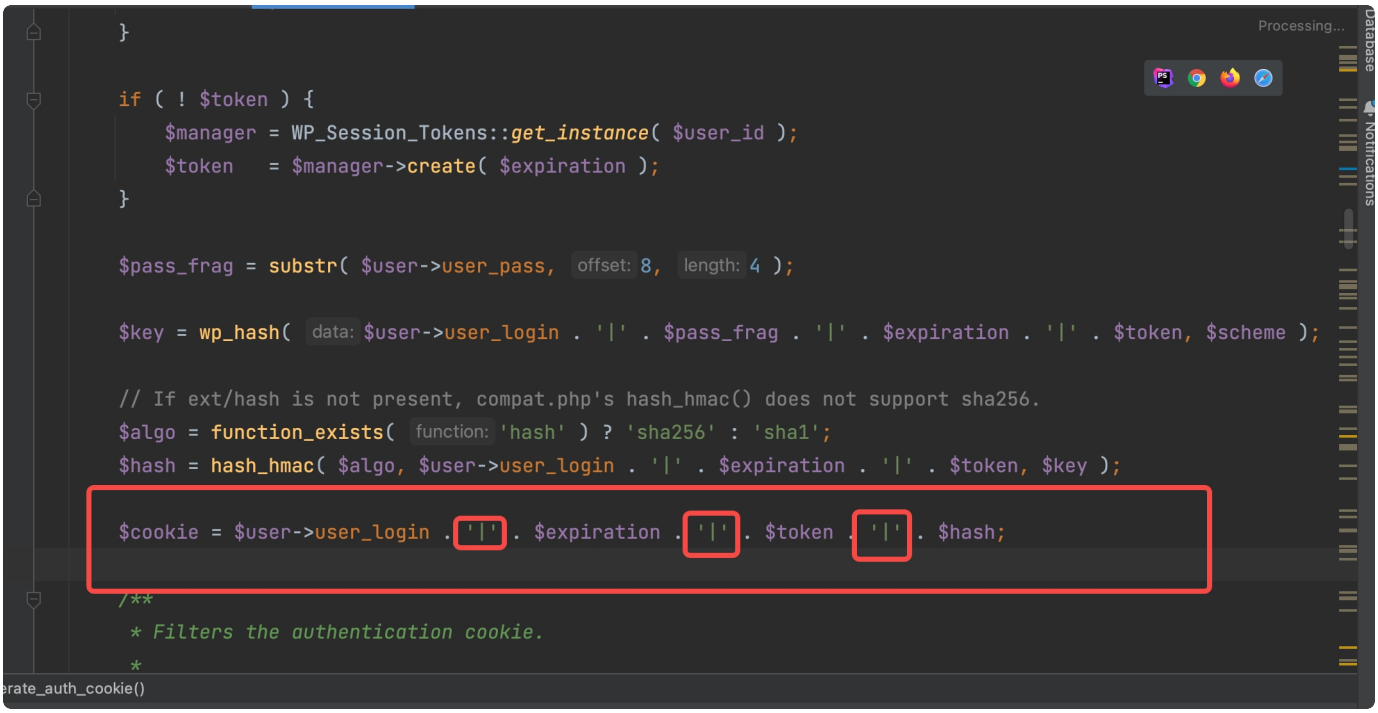
漏洞分析

该漏洞的原因很简单，由于在Modern Events Calendar Lite v5.16.5版本对该漏洞进行了修复，我们可以对比5.17版本和5.16.2版本的diff，看是如何修复的。

```
                $file_name = md5($post_id).'.'.$this->main->get_image_type
                $path = rtrim($wp_upload_dir['path'], DS.' ').DS.$file_nam
                $url = rtrim($wp_upload_dir['url'], '/ ').'/'.$file_name;
                $file->write($path, $photo);
                $this->main->set_featured_image($url, $post_id);
            }
        }
        return array('success'=>1, 'data'=>$post_ids);
    }
    public function export_all_events_do()
    {
+       // Current User Doesn't Have Access
+       if(!current_user_can('mec_import_export')) return false;
        $format = isset($_GET['format']) ? sanitize_text_field($_GET['form
        $events = $this->main->get_events('-1');
        // MEC Render Library
        $render = $this->getRender();
        switch($format)
        {
            case 'ical':
```

5.17版本比5.16版本在export_all_event_do函数多出了导出前判断当前用户权限的操作。所以如果请求中无代表当前用户身份的字段，则可判断为攻击。

wordpress中cookie身份设置如下，可见会存在三个"|"



```
    }

    if ( ! $token ) {
        $manager = WP_Session_Tokens::get_instance( $user_id );
        $token   = $manager->create( $expiration );
    }

    $pass_frag = substr( $user->user_pass, offset: 8, length: 4 );

    $key = wp_hash( data: $user->user_login . '|' . $pass_frag . '|' . $expiration . '|' . $token, $scheme );

    // If ext/hash is not present, compat.php's hash_hmac() does not support sha256.
    $algo = function_exists( function: 'hash' ) ? 'sha256' : 'sha1';
    $hash = hash_hmac( $algo, $user->user_login . '|' . $expiration . '|' . $token, $key );

    $cookie = $user->user_login . '|' . $expiration . '|' . $token . '|' . $hash;

    /**
     * Filters the authentication cookie.
     *
erate_auth_cookie()
```

规则解析

1. 提取特征点：url参数以及cookies部分
2. 特征点原因：该漏洞触发url以及参数固定，cookie如果不带有标明当前用户身份信息的字段则可判断为攻击
3. 规则：http.url*^"wp-admin/admin.php?"&&http.url*^sequence("page","=","MEC-ix")&&http.url*^sequence("tab","=","MEC-export")&&http.url*^sequence("mec-ix-action","=","export-events")&&http.url*^sequence("format","=")&&urldec(http.cookie)!~"wordpress_[0-9a-zA-Z]+=.+\|.+\|.+\|"
4. 最佳检测方案：使用规则进行检测。