漏洞分析 | 通达 OA 文件包含 & 文件上传漏洞分析

漏洞背景

近日，HSCERT 监测发现通达 OA 在官方论坛发布了紧急通告，提供了针对部分用户反馈遭到勒索病毒攻击的补丁更新，遭受攻击的 OA 服务器首页被恶意篡改，伪装成 OA 系统错误提示页面让用户下载安装插件，同时服务器上文件被勒索病毒重命名并加密。

遭受勒索的具体现象是：主页被篡改、站点文件扩展名被修改、生成一个勒索提示文本文件。

漏洞分析

从官网下载的补丁发现程序对 / ispirit/im/upload.php 文件进行了修改，着重分析该文件未修复前的代码：

```php
$P = $_POST['P'];
if (isset($P) || $P != '') {
    ob_start();
    include_once 'inc/session.php';
    session_id($P);
    session_start();
    session_write_close();
} else {
    include_once './auth.php';
}
```

在 $_POST['P'] 不为空的情况下，包含 inc/session.php 进行用户的 session 操作，否则就包含 /auth.php 进行用户鉴权。

```php
if (1 <= count($_FILES)) {
    if ($UPLOAD_MODE == '1') {
        if (strlen(urldecode($_FILES['ATTACHMENT']['name'])) !=
        strlen($_FILES['ATTACHMENT']['name'])) {
            $_FILES['ATTACHMENT']['name'] = urldecode($_FILES[
            'ATTACHMENT']['name']);
        }
    }
    $ATTACHMENTS = upload('ATTACHMENT', $MODULE, false);
```

当请求中存在文件上传时调用 upload 函数进行处理，在该函数中：

```
if (!is_uploadable($ATTACH_NAME)) {
    $ERROR_DESC = sprintf(_(
    '禁止上传后缀名为[%s]的文件'), substr(
    $ATTACH_NAME, strrpos($ATTACH_NAME, '.') + 1));
}
```

通过 is_uploadable 函数：

```
$POS = strrpos($FILE_NAME, '.');
if ($POS === false) {
    $EXT_NAME = $FILE_NAME;
} else {
    if (strtolower(substr($FILE_NAME, $POS + 1, 3)) ==
    'php') {
        return false;
    }
    $EXT_NAME = strtolower(substr($FILE_NAME, $POS + 1));
}
if (find_id(MYOA_UPLOAD_FORBIDDEN_TYPE, $EXT_NAME)) {
    return false;
}
```

判断 $_FILES['ATTACHMENT']['name'] 是否是允许上传的文件类型，禁止上传 php 文件且上传后的文件在 / attach/ 目录不能直接访问。

所以还需要找到一个文件包含漏洞来实现最终的 getshell。

文件 /ispirit/interface/gateway.php 中有个文件包含：

```php
if ($url != '') {
    if (substr($url, 0, 1) == '/') {
        $url = substr($url, 1);
    }
    if (strpos($url, 'general/') !== false || strpos($url,
    'ispirit/') !== false || strpos($url, 'module/') !==
    false) {
        include_once $url;
    }
}
```

而这个 $url 来源于 $json 数组：

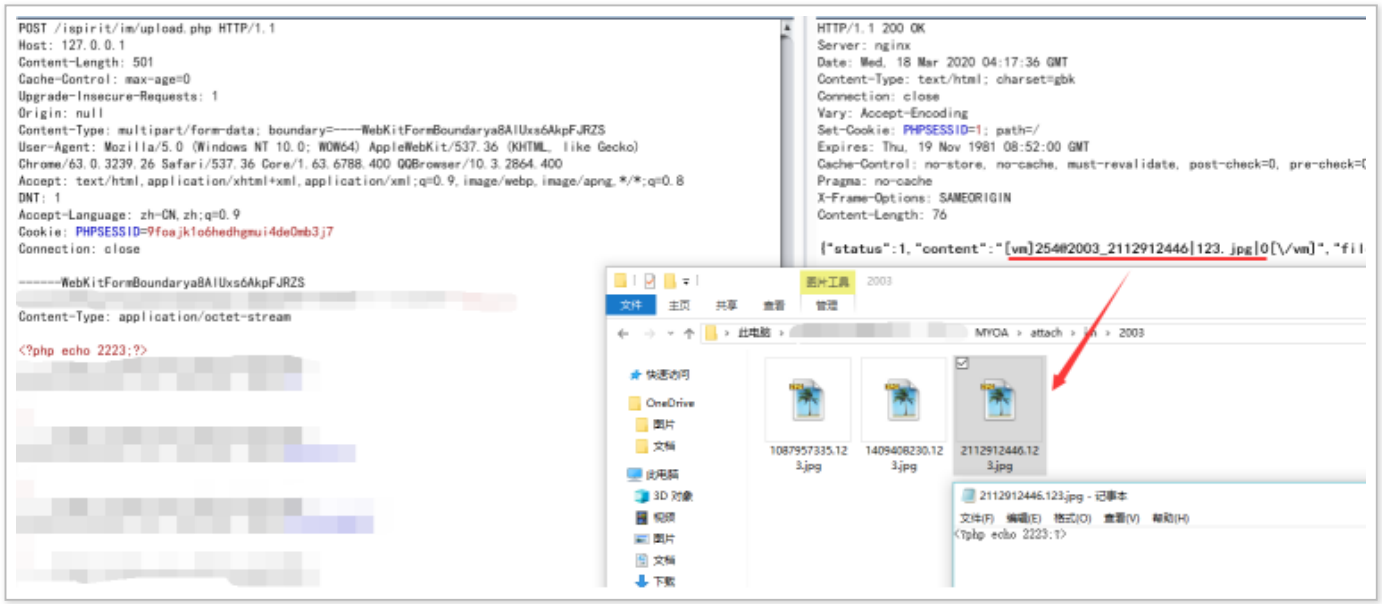
```php
$json = stripcslashes($json);
$json = (array) json_decode($json);
foreach ($json as $key => $val) {
    if ($key == 'data') {
        $val = (array) $val;
        foreach ($val as $keys => $value) {
            ${$keys} = $value;
        }
    }
    if ($key == 'url') {
        $url = $val;
    }
}
```

并且当 $_GET['P'] 为空的情况下就不进行权限校验：

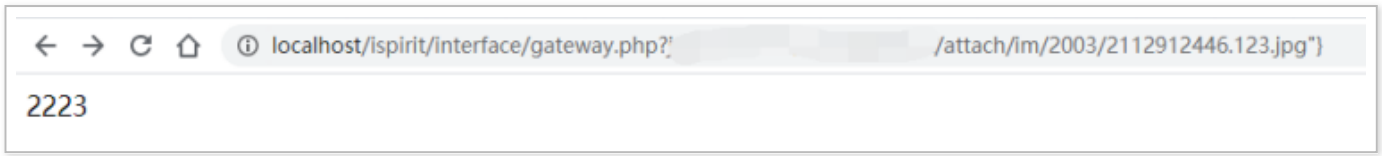
```php
if ($P != '') {
    if (preg_match('/[^a-z0-9;]+/i', $P)) {
        echo _('非法参数');
        exit;
    }
    session_id($P);
    session_start();
    session_write_close();
    if ($_SESSION['LOGIN_USER_ID'] == '' || $_SESSION[
    'LOGIN_UID'] == '') {
        echo _('RELOGIN');
        exit;
    }
}
```

综上，通过 /ispirit/im/upload.php 上传包含 php 代码的. jpg 文件，通过 /ispirit/interface/gateway.php 来包含该文件可实现最终的 getshell，也可以通过 /ispirit/interface/gateway.php 的包含漏洞直接包含日志文件来实现 getshell。

文件上传漏洞复现：



文件包含后执行结果：



漏洞危害

高危

影响版本

V11 版（文件包含漏洞只存在于此版本）

2017 版

2016 版

2015 版

2013 增强版

2013 版

安全建议

根据已知的恶意攻击风险，建议尽快测试更新补丁：

V11 版：

http://cdndown.tongda2000.com/oa/security/2020_A1.11.3.exe
2017 版：

http://cdndown.tongda2000.com/oa/security/2020_A1.10.19.exe
2016 版：

http://cdndown.tongda2000.com/oa/security/2020_A1.9.13.exe
2015 版：

http://cdndown.tongda2000.com/oa/security/2020_A1.8.15.exe
2013 增强版：

http://cdndown.tongda2000.com/oa/security/2020_A1.7.25.exe

2013 版：

http://cdndown.tongda2000.com/oa/security/2020_A1.6.20.exe

参考信息

http://club.tongda2000.com/forum.php?mod=viewthread&tid=128377&extra=page%3D1