



HACKING HOTSPOTS

***Pre-AUTH RCE, ARBITRARY SMS & ADJACENT
ATTACKS ON 5G AND LTE ROUTERS***

AGenda

whoami

Related Work

Tuoshi 5G & 4G routers

Kuwfi 5G & LTE routers

Demos

Conclusions



WHOami



Sr. Cybersecurity Analyst

F500

Former Information Security Analyst

 SEDARA™

Previous Talks:



Related Work

ZTE MF910 - Web Interface Black Box

All requests which “do something” are made to `/goform/*` API endpoints.

- `/goform/goform_get_cmd_process`
 - For reading data.
- `/goform/goform_set_cmd_process`
 - For writing data.



Related Work

Tuoshi 5G CPE Router NR500-EA udx710 unlocking help!? #55

 Closed Unanswered Preservio asked this question in Q&A



Preservio on Feb 5, 2024

edited ▼ ...

Hello, i have recently bought Tuoshi 5G CPE Router NR500-EA from aliexpress. I am very new to android or unlocking bootloader/customRoms.

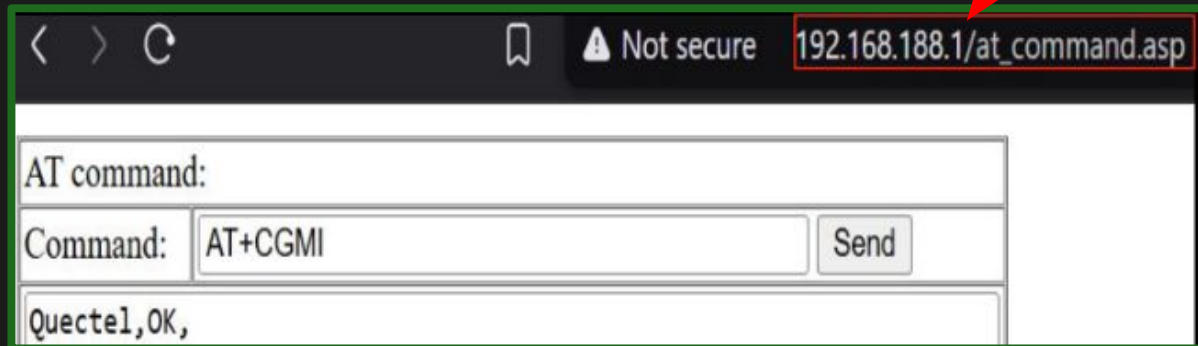
The UI is very buggy and has hidden menus that i was able to find via browsers developer mode. One Menu is called debug mode, which has USB mode and Debugging mode on/off. However when i turn these on i am not sure if it does any thing, adb & fastboot can't connect to it.

SSH is also enabled by default, i cannot login as root or admin and have tried the ui/wifi passwords which do not work. I am able to login as 'user' where the host name shows up as 'udx710'. With the user account i can't really do anything as most apps in /bin/ are locked down and 'user' doesn't have permissions to use them (simple system apps like ls & pwd).

Related Work

Name	Description
CVE-2024-48442	Incorrect access control in Shenzhen Tuoshi Network Communications Co.,Ltd 5G CPE Router NR500-EA RG500UEAABxCOMSLICv3.2.2543.12.18 allows attackers to access the SSH protocol without authentication.
CVE-2024-48440	Shenzhen Tuoshi Network Communications Co.,Ltd 5G CPE Router NR500-EA RG500UEAABxCOMSLICv3.2.2543.12.18 was discovered to contain a command injection vulnerability via the component at <code>command.asp</code> .

 medium.com/@sengkyaut



< > ↻ Not secure 192.168.188.1/at_command.asp

AT command:

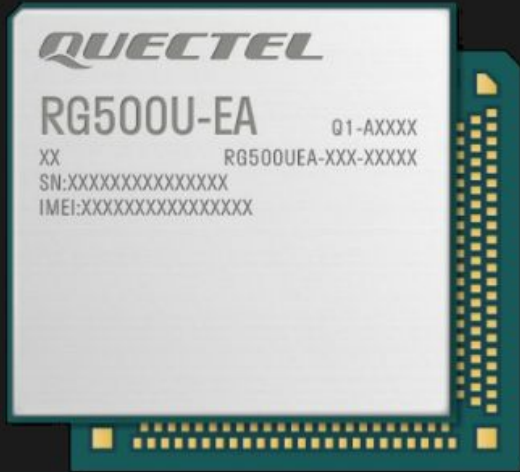
Command:

Quectel,OK,

Shenzhen Tuoshi Network, Communications Co.,LTD

Model: 5G CPE Router NR500-EA

Quectel RG500U Series 5G Chip



Search Results

There are **743** CVE Records that match your search.

Name	Description
CVE-2025-22949	Tenda ac9 v1.0 firmware v15.03.05.19 is vulnerable to command injection in <code>/goform/SetSambaCfg</code> , which may lead to arbitrary code execution.
CVE-2025-22946	Tenda ac9 v1.0 firmware v15.03.05.19 contains a stack overflow vulnerability in <code>/goform/SetSambaCfg</code> , which may lead to remote arbitrary code execution.
CVE-2025-22912	RE11S v1.11 was discovered to contain a buffer overflow vulnerability in <code>/goform/SetSambaCfg</code> , which may lead to arbitrary code execution.
CVE-2025-22906	RE11S v1.11 was discovered to contain a buffer overflow vulnerability in <code>/goform/SetSambaCfg</code> , which may lead to arbitrary code execution.
CVE-2025-22905	RE11S v1.11 was discovered to contain a buffer overflow vulnerability in <code>/goform/SetSambaCfg</code> , which may lead to arbitrary code execution.
CVE-2025-0566	A vulnerability classified as critical has been found in Tenda AC5 15.03.06.47 and classified as critical has been disclosed to the public and may be used.
CVE-2025-0528	A vulnerability, which was classified as critical has been found in Tenda AC5 15.03.06.47 and classified as critical has been disclosed to the public and may be used.
CVE-2025-0349	A vulnerability classified as critical has been found in Tenda AC5 15.03.06.47 and classified as critical has been disclosed to the public and may be used.
CVE-2024-9915	A vulnerability classified as critical was found in Tenda AC5 15.03.06.47 and classified as critical has been disclosed to the public and may be used.
CVE-2024-9914	A vulnerability classified as critical has been found in Tenda AC5 15.03.06.47 and classified as critical has been disclosed to the public and may be used.
CVE-2024-9913	A vulnerability was found in D-Link DIR-619L 2.06B01 and classified as critical has been disclosed to the public and may be used.

Search Results

There are **912** CVE Records that match your search.

Name	Description
CVE-2025-6887	A vulnerability was found in Tenda AC5 15.03.06.47 and classified as critical has been disclosed to the public and may be used.
CVE-2025-6886	A vulnerability has been found in Tenda AC5 15.03.06.47 and classified as critical has been disclosed to the public and may be used.
CVE-2025-6882	A vulnerability classified as critical has been found in D-Link DIR-513 1.10.0.0 and classified as critical has been disclosed to the public and may be used.
CVE-2025-6734	A vulnerability was found in UTT HiPER 840G up to 3.1.1-190328. It has been disclosed to the public and may be used.
CVE-2025-6733	A vulnerability was found in UTT HiPER 840G up to 3.1.1-190328. It has been disclosed to the public and may be used.
CVE-2025-6732	A vulnerability was found in UTT HiPER 840G up to 3.1.1-190328. It has been disclosed to the public and may be used.
CVE-2025-6617	A vulnerability was found in D-Link DIR-619L 2.06B01 and classified as critical has been disclosed to the public and may be used.
CVE-2025-6616	A vulnerability has been found in D-Link DIR-619L 2.06B01 and classified as critical has been disclosed to the public and may be used.

Top 10 CVE ID Count by Vendor

Edimax

1.3%

Embedthis GoAhead...

1.6%

Linksys

1.6%

Jensen of Scandinavia

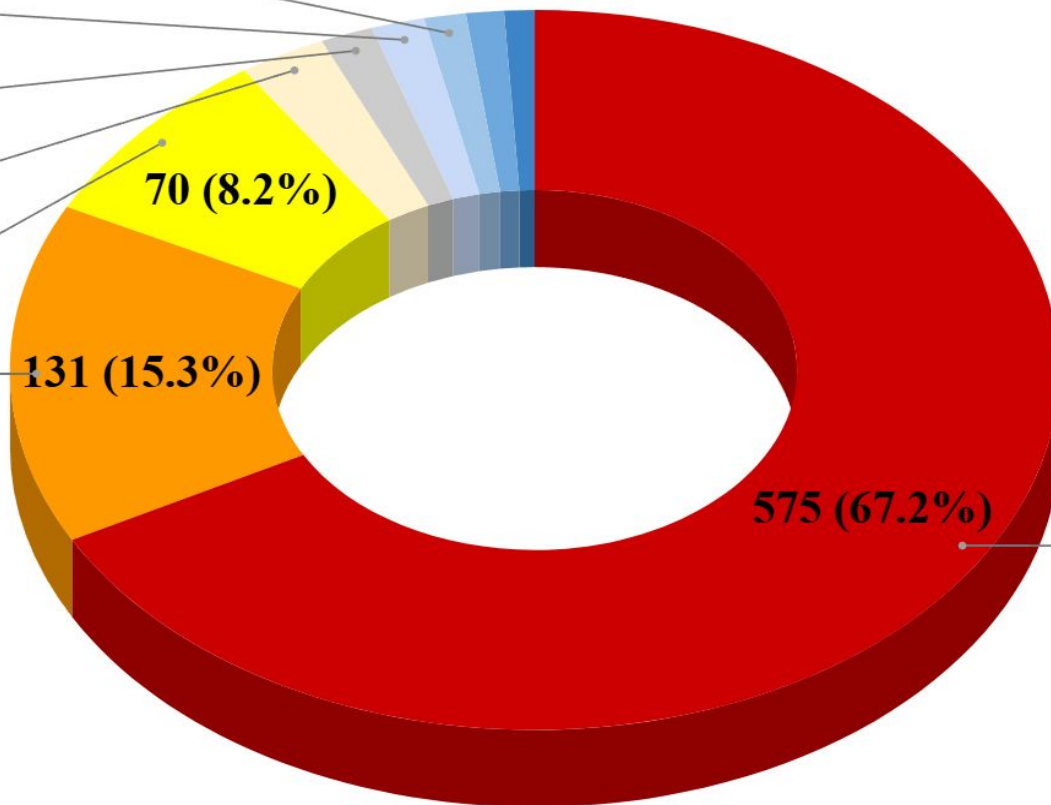
2.7%

H3C

8.2%

D-Link

15.3%



Tenda

67.2%

/goform/



username=admin;

Request

Pretty Raw Hex

```
1 POST /goform/ formJsonAjaxReq HTTP/1.1
2 Host: 192.168.188.1
3 Content-Length: 118
4 X-Requested-With: XMLHttpRequest
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
6 Accept: application/json, text/javascript, */*; q=0.01
7 Content-Type: application/json
8 Sec-GPC: 1
9 Origin: http://192.168.188.1
10 Referer: http://192.168.188.1/home.asp
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: userLanguage=EN; ace_settings=%7B%22sidebar-collapsed%22%3A1%7D;
  username=admin; first_login=Fl
14 Connection: keep-alive
15
16 {
  "action": "set_timesetting",
  "data": {
    "ntpserver0": "ntp1.aliyun.com",
    "ntpserver1": "ntp2.aliyun.com",
    "timezone": "UTC-8"
  }
}
```

%7B%22sidebar-collapsed%22%3A1%7D ≠ session token

Decompile: FUN_0043052c - (jhttp2)

```
21  iVar2 = cJSON_GetObjectItem(param_2,"ntpserver0");
22  if (iVar2 != 0) {
23      pcVar9 = *(char **) (iVar2 + 0x10);
24      pcVar3 = (char *)nvram_safe_get("ntp_server0");
25      iVar2 = strcmp(pcVar9,pcVar3);
26      if (iVar2 != 0) {
27          nvram_set("ntp_server0",pcVar9);
28          nvram_modified = 1;
29          do_system("echo -n \"%s\" >/tmp/NTPServerIP",pcVar9);
30          bVar1 = true;
31          goto LAB_00430600;
32      }
33  }
34  bVar1 = false;
35 LAB_00430600:
36  iVar2 = cJSON_GetObjectItem(param_2,"ntpserver1");
37  if (iVar2 != 0) {
38      pcVar9 = *(char **) (iVar2 + 0x10);
39      pcVar3 = (char *)nvram_safe_get("ntp_server1");
40      iVar2 = strcmp(pcVar9,pcVar3);
41      if (iVar2 != 0) {
42          nvram_set("ntp_server1",pcVar9);
43          bVar1 = true;
44          nvram_modified = 1;
45      }
```

```
nvram_set("ntp_server0",pcVar9);
nvram_modified = 1;
do_system("echo -n \"%s\" >/tmp/N
```



DEMO I


```
sh-5.0# cat /etc/shadow
cat /etc/shadow
root:abjNLSdNYTy/6:19898:0:99999:7:::
daemon*:19898:0:99999:7:::
bin*:19898:0:99999:7:::
sys*:19898:0:99999:7:::
sync*:19898:0:99999:7:::
games*:19898:0:99999:7:::
man*:19898:0:99999:7:::
lp*:19898:0:99999:7:::
mail*:19898:0:99999:7:::
news*:19898:0:99999:7:::
uucp*:19898:0:99999:7:::
proxy*:19898:0:99999:7:::
www-data*:19898:0:99999:7:::
backup*:19898:0:99999:7:::
list*:19898:0:99999:7:::
irc*:19898:0:99999:7:::
gnats*:19898:0:99999:7:::
messagebus!:19898:0:99999:7:::
sshd!:19898:0:99999:7:::
radvd!:19898:0:99999:7:::
ntp!:19898:0:99999:7:::
www!:19898:0:99999:7:::
user::19898:0:99999:7:::
nobody*:19898:0:99999:7:::
```

abjNLSdNYTy/6

admin!2#

HTTP 80/TCP

01/25/2025 14:59 UTC

BOOTSTRAP

JQUERY

Details

http://[REDACTED]

[VIEW ALL DATA](#)[↗ GO](#)**Status** 200 OK**Body Hash** sha1:42ff1b85[REDACTED]5f008c65ae69**HTML Title** NR Router**Response Body**[EXPAND](#)

HTTP 7547/TCP

01/24/2025 20:03 UTC

Details

http://[REDACTED]:7547/

[VIEW ALL DATA](#)[↗ GO](#)**Status** 401 Unauthorized

SSH 10022/TCP


01/24/2025 18:00 UTC


REMOTE ACCESS



 User Login

English 

Username 

Password 

 Login

LTE/4G

Tuoshi, AKA "DIONLINK"

Model: LT15D & LT21B



<http://www.tuoshi.net/productview.asp?id=226>
<http://www.tuoshi.net/productview.asp?id=218>
<http://amazon.com/s?k=dionlink>



Home > Network Setting > Online Checker

Online Checker » Online Monitor Setup

Online Keeper Switch ☒ ON

Check IP Address 1 \$(reboot)

Check IP Address 2 8.8.8.8

Check interval (s) 10

Offline Time (min) 30

☐ Whether to reboot automatically if offline

Decompile: UndefinedFunction_00426300 - (jhttpd_dionlink)

```
1
2 void UndefinedFunction_00426300(undefined4 param_1,int param_2)
3
4 {
5     int iVar1;
6     char *pcVar2;
7     int iVar3;
8     char *pcVar4;
9
10    if (param_2 != 0) {
11        iVar1 = cJSON_GetObjectItem(param_2,"check_ip1");
12        if (iVar1 != 0) {
13            pcVar4 = *(char **) (iVar1 + 0x10);
14            pcVar2 = (char *)nvrn_safe_get("network_check_ip1");
15            iVar1 = strcmp(pcVar4,pcVar2);
16            if (iVar1 != 0) {
17                nvrn_set("network_check_ip1",pcVar4);
18                nvrn_modified = 1;
19                do_system("echo -n \"%s\" >/tmp/network_check_ip1",pcVar4);
20            }
21        }
22        iVar1 = cJSON_GetObjectItem(param_2,"check_ip2");
23        if (iVar1 != 0) {
24            pcVar4 = *(char **) (iVar1 + 0x10);
25            pcVar2 = (char *)nvrn_safe_get("network_check_ip2");
26            iVar1 = strcmp(pcVar4,pcVar2);
27            if (iVar1 != 0) {
28                nvrn_set("network_check_ip2",pcVar4);
29                nvrn_modified = 1;
30                do_system("echo -n \"%s\" >/tmp/network_check_ip2",pcVar4);
31            }
32        }
33    }
```

do_system("echo -n \"%s\" >/tmp/network_check_ip1",pcVar4);

CVE-2024-53931



DEMO II

KUWFI

Model: GC111, AC900
& CPF908

4G/ LTE Routers



Model: GC111

LTE/4G



```
__stack_chk_guard;
```

CVE-2025-43984

CVE-2025-43985

CVE-2025-43986

Architecture: ARM EABI5 (hard-wired to run on ARMv5- style cores)
No address- space randomization (fixed load address)
Format: ELF 32-bit LSB shared object (non-PIE)

String Search [CodeBrowser: Kuwfi:/kthy_topsw_goahead]

String Search - 1 items (of 3034) - [kthy_topsw_goahead, Minimum size = 5, Align = 1]

Location	String View	String Type
0007a324	"ctrl_interface=/var/run/wpa_supplicant\nctrl_interface_group=0\n\nnetwork={\nkey_mgmt=NO\nssid=\"%s\"\n}\n"	string

Decompile: UndefinedFunction_00058580 - (kthy_topsw_goahead)

```
40 sprintf(__s, "%s/%s", param_1, __s_00);
41 FUN_000574e4(__s);
42 iVar2 = access(__s, 0);
43 if (iVar2 == 0) {
44     kthy_log_append("../kthy_web/kthy_httpshare_process.c", 0x216, "kthy_httpshare.log",
45                     " del file fail");
46 }
```

Decompile: FUN_000574e4 - (kthy_topsw_goahead)

```
1
2 undefined4 FUN_000574e4(char *param_1)
3
4 {
5     size_t sVar1;
6     char *__s;
7
8     if (param_1 != (char *)0x0) {
9         sVar1 = strlen(param_1);
10        __s = (char *)malloc(sVar1 + 10);
11        __s[0] = '\0';
12        __s[1] = '\0';
13        __s[2] = '\0';
14        __s[3] = '\0';
15        sprintf(__s, "rm -rf \'%s\'", param_1);
16        kthy_log_append("../kthy_web/kthy_httpshare_process.c", 0x17, "kthy_httpshare.log",
17                        "kthy_httpshare_call_system: [%s] \n", __s);
18        system(__s);
19        free(__s);
20        return 1;
21    }
22    sprintf(__s, "rm -rf \'%s\'", param_1);
23    kthy_log_append("../kthy_web/kthy_httpshare_process.c", 0x17, "kthy_httpshare.log",
24                    "kthy_httpshare_call_system: [%s] \n", __s);
25    system(__s);
26    free(__s);
27    return 1;
28 }
```

ssid

FUN_000574e4

system(__s)



DEMO III

Model: AC900

LTE/4G



CVE-2024-53945

CVE-2024-53946

SoC (System on Chip):

CPU: MT7621+MT7603E+MT7612E

Flash: 16MB Flash

RAM: 128MB DDR3 RAM

```
58 callShell(acStack_4c0,auStack_43c,0x400);
```

Pretty	Raw	Hex
--------	-----	-----

[illegible]



DEMO IV & V

Model: CPF908

LTE/4G



<https://fcc.report/FCC-ID/2AX9H-25126/5081635>

https://m.media-amazon.com/images/I/61eE90YzOQL._AC_SL1500_.jpg

8.3.	AT+CSCA	Service Center Address	134
8.4.	AT+CPMS	Preferred Message Storage	135
8.5.	AT+CMGD	Delete Messages	137
8.6.	AT+CMGL	List Messages.....	138
8.7.	AT+CMGR	Read Messages.....	142
8.8.	AT+CMGS	Send Messages.....	145
8.9.	AT+CMMS	Send More Messages.....	147
8.10.	AT+CMGW	Write Messages to Memory	148
8.11.	AT+CMSS	Send Messages from Storage.....	150



DEMO VI

KUWFI

MODEL:
5G ROUTER
5G01-X55

Chipset:
Snapdragon X62





DEMO VII



DEMO VIII

conclusions

1. CWE-284: Improper Access Control
2. CWE-200: Information Disclosure
3. CWE-287: Improper Authentication
4. CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
5. CWE-352: Cross-Site Request Forgery (CSRF)



THANK YOU!

