

KT_GIGA_WIFI-Wave 2 has a stack overflow vulnerability

The device information is as follows



designed by **kt**

제품명 GIGA WiFi Wave 2

제조국 중국

모델명 KM08-708H

제조년월 2017.09

제조사 (주)머큐리

정격 12V \approx 2.1A / 2A

무선랜명 **KT_GIGA_5G_3CA5**

암호키 **4cdc1kd588**

- 암호키는 노출될 수 있으니 변경 후 사용할 것을 권합니다.
- 상하에 다른 기기를 겹쳐 사용하지 마세요.

MAC ADDRESS **883C1C503CA5**

제조관리번호 **201709183588**

KT BARCODE **GHAP9191041183588**



MSIP-CMM-MCS
-KM08-708H

A/S센터 1566-5202

고객센터 국번없이 100번

본 제품은 (주)KT의 자산으로, 서비스 해지 시 반납하셔야 합니다.

- KT에서 제공하는 장비는 기능 고도화 및 서비스 향상을 위해 원격으로 관리, 제어될 수 있음
- 해당 무선 장비는 운용 중 전파 혼선 가능성이 있음
- 이 장치는 보안성이 약해 타사 인터넷전화 사용 시 도청가능성이 있음

According to the web interface, the firmware version is KM08-708H 1.1.14

☆ 상태정보

| 시스템 정보

| 유무선 연결 정보

| 유무선 단말 정보

| 로그 정보

☆ 간편개통설정 (2.4GHz)

☆ 간편개통설정 (5GHz)

☆ 장치설정

시스템정보

장비명	홈브
모델명/제조사	KM08-708H/MERCURY
버전	1.1.14
날짜/시간	Jan 1 10:03:28
시스템업타임	0 Day(s) 1 Hour(s) 3 Minute(s) 29 Second(s) Elapsed
메모리사용량	15%
CPU 사용량	5Sec:3% / 1Min: 1% / 10Min:0%
대표 MAC 주소	88:3C:1C:50:3C:A5

인터넷 연결정보

인터페이스	WAN
IP 할당 방식	DHCP
IP주소	0.0.0.0
서브넷마스크	0.0.0.0
게이트웨이	0.0.0.0
기본 DNS	168.126.63.1
보조 DNS	0.0.0.0

LAN 연결 정보

IP 할당 정책	kt 모드
DHCP 서버	활성
IP 주소	172.30.1.254
서브넷마스크	255.255.255.0
코넷 DHCP IP 범위	172.30.1.1 ~ 172.30.1.60
프리미엄 DHCP IP 범위	172.30.1.128 ~ 172.30.1.148
DHCP 임대시간(sec)	3600

In the goahead binary program, a stack overflow vulnerability can be observed in the websRedirect function

```

1 int __fastcall websRedirect(int a1, const char *haystack)
2 {
3     const char *v5; // $s0
4     const char *Var; // $s3
5     int mcr_userPort; // $s2
6     const char *haystack_1; // [sp+20h] [-105Ch] BYREF
7     int v9; // [sp+24h] [-1058h] BYREF
8     char s[4180]; // [sp+28h] [-1054h] BYREF
9
10    memset(s, 0, 0x1050u);
11    haystack_1 = 0;
12    v9 = 0;
13    ++dword_48BCCC;
14    if ( !strstr(haystack, "http://") )
15    {
16        v5 = &haystack[*haystack == 0x2F];
17        Var = (const char *)_websGetVar__(a1, "HTTP_HOST", websHostUrl);
18        mcr_userPort = mcr_userPort;
19        if ( mcr_userPort == 80 || strchr(Var, 58) )
20            strcpy(s, Var);
21        else
22            sprintf(s, "%s:%d", Var, mcr_userPort);
23        fmtAlloc(&haystack_1, 4176, "http://%s/%s", s, v5);
24        haystack = haystack_1;
25    }
26    fmtAlloc(
27        &v9,
28        4176,
29        "<html><head></head><body>\r\n"
30        "\t\t\tThis document has moved to a new <a href=\"%s\">location</a>.\r\n"
31        "\t\t\tPlease update your documents to reflect the new location.\r\n"
32        "\t\t</body></html>\r\n",
33        haystack);
34    if ( *(_DWORD *) (a1 + 248) == 80 )
35        websResponse(a1, 301, v9, haystack);
36    else
37        websResponse(a1, 302, v9, haystack);
38    bfreeSafe(v9);
39    return bfreeSafe(haystack_1);
40 }

```

The request package for burpsuit construction is as follows

代码块

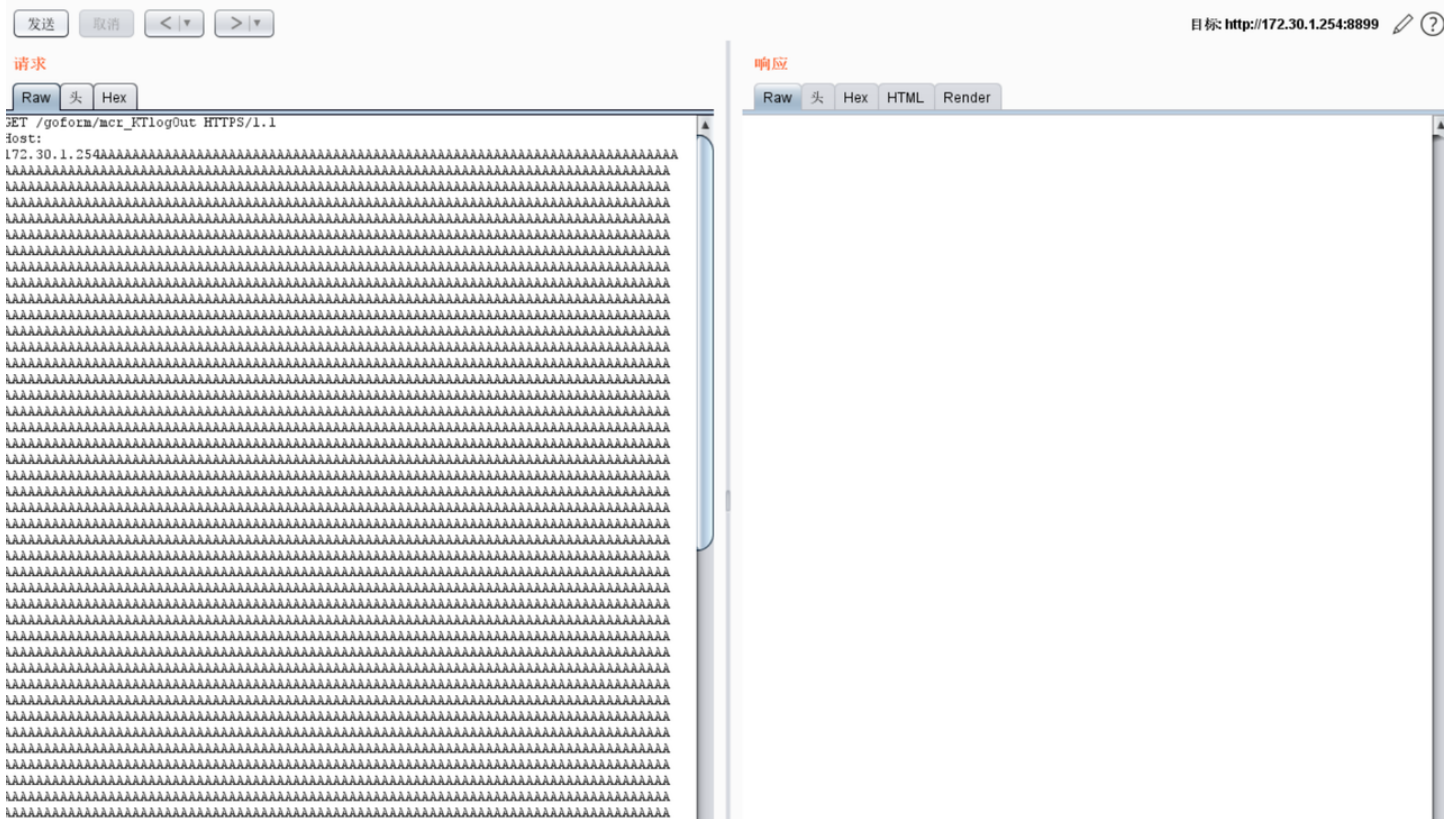
[illegible]

[illegible]

[illegible]

```
3 User-Agent: test
4 Accept: */*
5 Connection: close
```

The purpose of using Burpsuit here is because Burpsuit can recognize the actual IP address of the target



Web service crashes successfully

