Vendor of the products: Tenda

Affected products: Tenda RX3 US_RX3V1.0br_V16.03.13.11_multi_TDE01

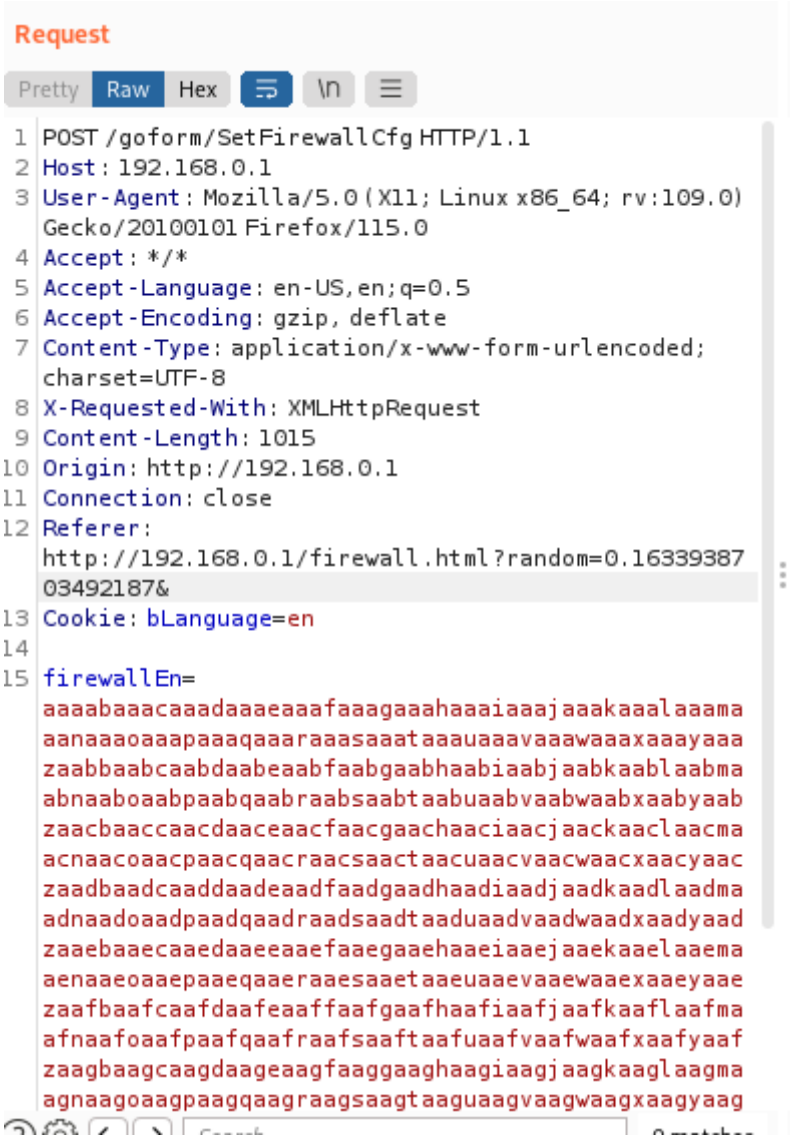
Hardware Link: https://www.tendacn.com/tw/download/detail-3980.html

Vulnerability Description

A buffer overflow vulnerability was discovered in Tenda RX3 US_RX3V1.0br_V16.03.13.11_multi_TDE01, triggered by the firewallEn parameter at /goform/SetFirewallCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.

POC

send



You can see that the router has crashed.

```
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
zsh: segmentation fault  sudo chroot ./ ./qemu-arm-static ./bin/httpd
```

Code in httpd

n the `formSetFirewallCfg` function, the value of `firewalEn` is retrieved and stored into `v4`. Subsequently, the value is copied into `firewall_buf` using `strcpy` without performing any safety checks, leading to a buffer overflow vulnerability.

```
1  void __fastcall formSetFirewallCfg(webs_t wp, char_t *path, char_t *query)
2  {
3    char_t *v4; // r4
4    size_t v5; // r0
5    char_t *fmt; // [sp+0h] [bp-58h]
6    char_t *fmta; // [sp+0h] [bp-58h]
7    unsigned __int8 firewall_buf[8]; // [sp+8h] [bp-50h] BYREF
8    unsigned __int8 old_wan_ping_buf[8]; // [sp+10h] [bp-48h] BYREF
9    unsigned __int8 old_ddos_buf[64]; // [sp+18h] [bp-40h] BYREF
10   unsigned __int8 mib_value[64]; // [sp+58h] [bp+0h] BYREF
11
12   *(_DWORD *)firewall_buf = 0;
13   *(_DWORD *)&firewall_buf[4] = 0;
14   memset(old_ddos_buf, 0, sizeof(old_ddos_buf));
15   *(_DWORD *)old_wan_ping_buf = 0;
16   *(_DWORD *)&old_wan_ping_buf[4] = 0;
17   memset(mib_value, 0, sizeof(mib_value));
18   v4 = websGetVar(wp, (char_t *)"firewallEn", (char_t *)"1111");
19   v5 = strlen((const char *)v4);
20   if ( v5 > 3 )
21   {
22     strcpy((char *)firewall_buf, (const char *)v4);
23     GetValue("security.ddos.map", old_ddos_buf);
24     GetValue("firewall.pingwan", old_wan_ping_buf);
25     sprintf((char *)mib_value, "%c,1500;%c,1500;%c,1500", firewall_buf[0], firewall_buf[2], firewall_buf[1]);
26     SetValue("security.ddos.map", mib_value);
27     SetValue("firewall.pingwan", &firewall_buf[3]);
28     v5 = doSystemCmd("cfm post  netctrl ddos_ip_fence?op=6");
29   }
30   CommitCfm(v5);
31   websWrite(wp, fmt);
32   websWrite(wp, fmta);
33   websDone(wp, 200);
34 }
```