Tenda AC21(V16.03.08.15) has a Stack Buffer Overflow Vulnerability

Product

1. product information:
2. firmware download:

Affected version

V16.03.08.15

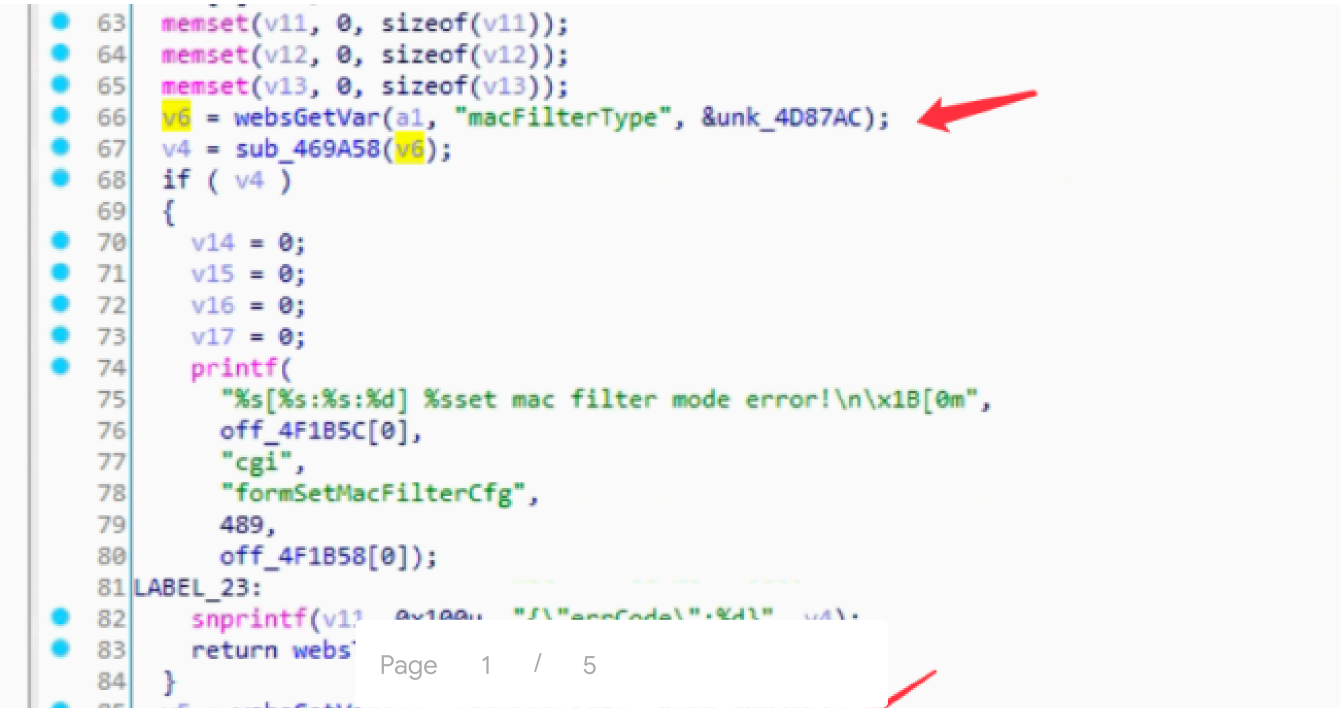
Vulnerability

The vulnerability is in /bin/httpd , the function `formSetMacFilterCfg`, which can be accessed via the URL `goform/setMacFilterCfg`.

Both `v6` and `v5` are externally accepted parameters.

Now is in `formSetMacFilterCfg` function.

Please notice the paramter `v5`, which is from the string `deviceList`.



```
memset(v11, 0, sizeof(v11));
memset(v12, 0, sizeof(v12));
memset(v13, 0, sizeof(v13));
v6 = websGetVar(a1, "macFilterType", &unk_4D87AC);
v4 = sub_469A58(v6);
if ( v4 )
{
  v14 = 0;
  v15 = 0;
  v16 = 0;
  v17 = 0;
  printf(
    "%s[%s:%s:%d] %sset mac filter mode error!\n\x1B[0m",
    off_4F1B5C[0],
    "cgi",
    "formSetMacFilterCfg",
    489,
    off_4F1B58[0]);
LABEL_23:
  snprintf(v11, 0x100u, "{\"errCode\":%d}", v4);
  return webs
}
```