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

Product

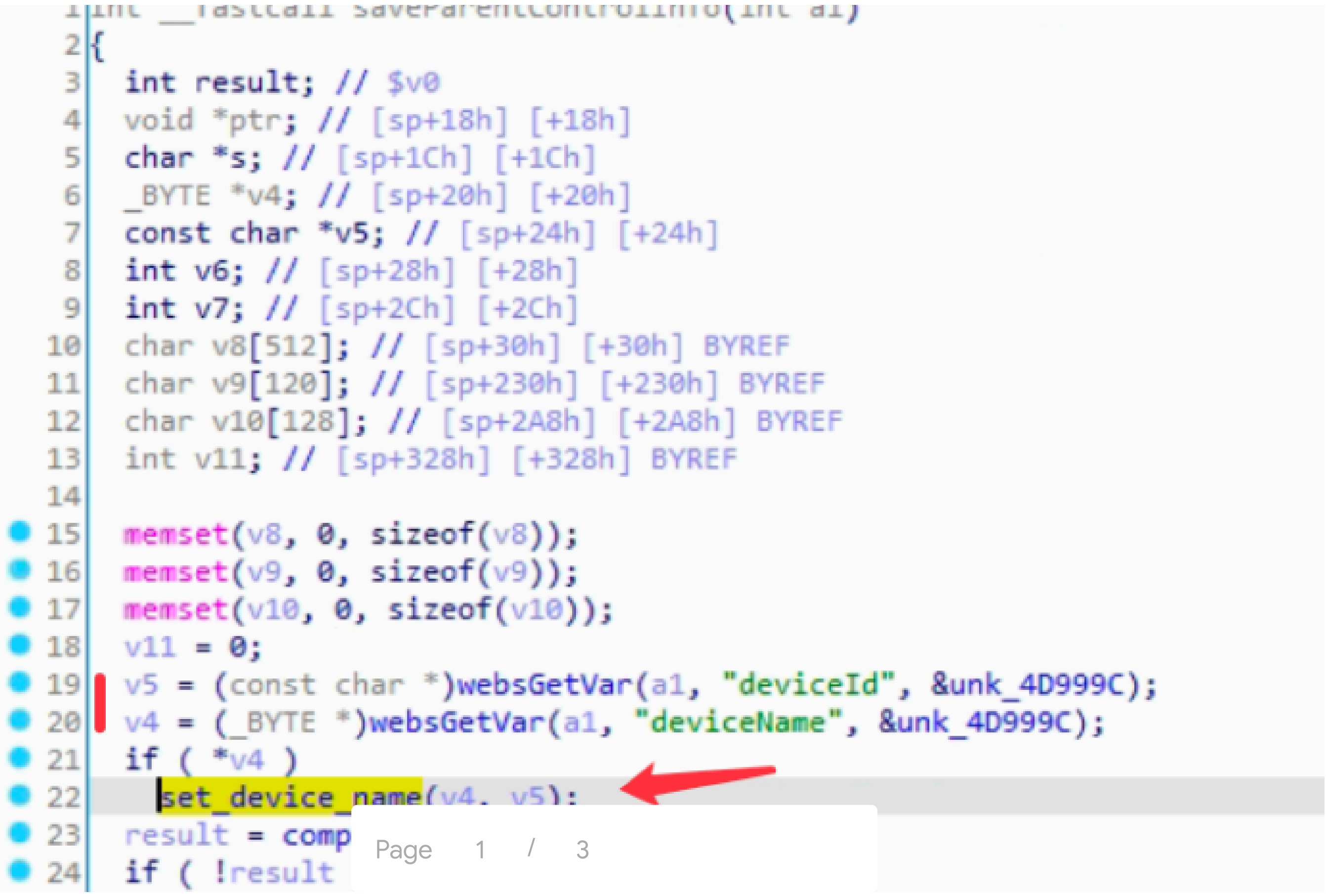
1. product information:
2. firmware download:

Affected version

V16.03.08.15

Vulnerability

The stack overfow vulnerability is in /bin/httpd. The vulnerability occurrs in the `set_device_name` function which can be accessed through the URL `goform/saveParentControlInfo`.



```
int __fastcall saveParentControlInfo(int a1)
{
  int result; // $v0
  void *ptr; // [sp+18h] [+18h]
  char *s; // [sp+1Ch] [+1Ch]
  _BYTE *v4; // [sp+20h] [+20h]
  const char *v5; // [sp+24h] [+24h]
  int v6; // [sp+28h] [+28h]
  int v7; // [sp+2Ch] [+2Ch]
  char v8[512]; // [sp+30h] [+30h] BYREF
  char v9[120]; // [sp+230h] [+230h] BYREF
  char v10[128]; // [sp+2A8h] [+2A8h] BYREF
  int v11; // [sp+328h] [+328h] BYREF

  memset(v8, 0, sizeof(v8));
  memset(v9, 0, sizeof(v9));
  memset(v10, 0, sizeof(v10));
  v11 = 0;
  v5 = (const char *)websGetVar(a1, "deviceId", &unk_4D999C);
  v4 = (_BYTE *)websGetVar(a1, "deviceName", &unk_4D999C);
  if ( *v4 )
    set_device_name(v4, v5);
  result = comp
  if ( !result
```