
RE: VMG5153-B30B 缓冲区溢出漏洞

3 封邮件

security <security@zyxel.com.tw>

2020年9月17日 下午6:20

收件人: 杨超 <firmianay@gmail.com>

抄送: security <security@zyxel.com.tw>

Hi楊超,

再次感謝您的通報，經內部驗證後確認存在有緩衝區溢出問題，但在VMG5313-B30B的原廠設定中，HTTP 遠端連線預設為關閉，況且產品本身有認證與隨機產生會話密鑰(session key) 的機制，因此風險較低。且VMG5313-B30B系列機種已EOL，根據產品EOL作業程序，我們將不再提供正式修補程式。謝謝!

Regards,

Zyxel Security Team

From: security**Sent:** Thursday, September 03, 2020 10:59 AM**To:** 杨超 <firmianay@gmail.com>**Cc:** security <security@zyxel.com.tw>**Subject:** RE: VMG5153-B30B 缓冲区溢出漏洞

Hi楊超,

感謝您的通報，我們會請相關團隊進行驗證，有任何進一步消息再與您聯繫，謝謝。

Regards,

Zyxel Security Team

From: 杨超 [<mailto:firmianay@gmail.com>]**Sent:** Wednesday, September 02, 2020 4:51 PM**To:** security <security@zyxel.com.tw>**Subject:** VMG5153-B30B 缓冲区溢出漏洞

你好，我在 VMG5313-B30B_5.11(ABCU.1)C0 中发现一个疑似缓冲区溢出，位于 zhttpd 程序的 FUN_00405218，该函数用于导入本地CA证书，URI 构造应该类似 "/cgi-bin/Certificates?action=import_local&priv=xxxxxxx"，由于程序采用 while 的方式寻找字符串 "xxxxxxx"的结尾 (&、?、\0)，然后直接与字符串开头相减作为 strncpy 函数的长度参数，如果字符串过长，可能导致溢出。

遗憾的是我没有真实设备进行测试，但我非常相信这个漏洞的存在，所以先发了这封邮件。期待你们的回复。

```
Decompile: FUN_00405218 - (zhhttpd)
14  undefined4 local_42c;
15  undefined4 local_428;
16  undefined4 local_424;
17  undefined4 local_420;
18  undefined4 local_41c;
19  undefined local_418;
20  char local_414 [1028];
21
22  bVar1 = false;
23  bVar2 = false;
24  local_42c = 0;
25  local_428 = 0;
26  local_424 = 0;
27  local_420 = 0;
28  local_41c = 0;
29  local_418 = 0;
30  memset(local_414,0,0x400);
31  local_444 = 1;
32  __haystack = (char *)cg_http_request_geturi(param_1);
33  local_44c = strstr(__haystack,"?action=import_local");
34  if (local_44c == (char *)0x0) {
35      local_44c = strstr(__haystack,"?action=import_ca");
36      if (local_44c != (char *)0x0) {
37          bVar1 = true;
38          local_450 = 0;
39      }
40  }
41  else {
42      bVar2 = true;
43      local_450 = 1;
44  }
45  if ((bVar1) || (bVar2)) {
46      if (bVar2) {
47          puts("Certificate Import: action=import_local, start to parse data...");
48          __haystack = strstr(local_44c + 0x14,"&priv=");
49          if (__haystack != (char *)0x0) {
50              local_44c = local_44c + 0x1a;
51              local_448 = local_44c;
52              while (((*local_448 != '&' && (*local_448 != '?')) && (*local_448 != '\0'))) {
53                  local_448 = local_448 + 1;
54              }
55              printf("Certificate Import: find &priv value, start=%d, end=%d.\n",local_44c,local_448);
56              if (local_448 != local_44c) {
57                  strncpy((char *)&local_42c,local_44c,(size_t)(local_448 - (int)local_44c));
58                  printf("Certificate Import: find private key password %s.\n",&local_42c);
59              }
60          }
61      }
62      iVar3 = cg_filelist_getBy_valname(*(undefined4 *) (param_1 + 0x26c),"certImportFileName");
63      if (iVar3 == 0) {
```

杨超 <firmianay@gmail.com>

2020年9月17日 下午8:00

收件人: security <security@zyxel.com.tw>

感谢回复，其实我是看过这篇文章（https://blog.somegeneric.ninja/Zyxel_VMG5153_B30B）后才下载的固件，那么这个问题是否也可以分配一个CVE呢？

security <security@zyxel.com.tw> 于2020年9月17日周四 下午6:20写道：
[引用文字已隐藏]

security <security@zyxel.com.tw>

2020年9月18日 上午9:55

收件人: 杨超 <firmianay@gmail.com>

抄送: security <security@zyxel.com.tw>

HI 楊超,

感謝您的回覆。關於CVE ID部分，因為漏洞是由您發現，建議由您申請會較為合適。若有任何問題，請再與我們聯絡，再次感謝您直接通報給Zyxel。

[引用文字已隐藏]