DCS-7517_B1_FW_v2.02.01 Weak Password Vulnerability

firmware version

- vendor: dlink_ipcamera
- product: DCS-7517B1
- version: below or equal v2.02.01
- firmware download url: https://files.dlink.com.au/products/DCS-7517/REV_B/Firmware/Firmware_2.02.01/

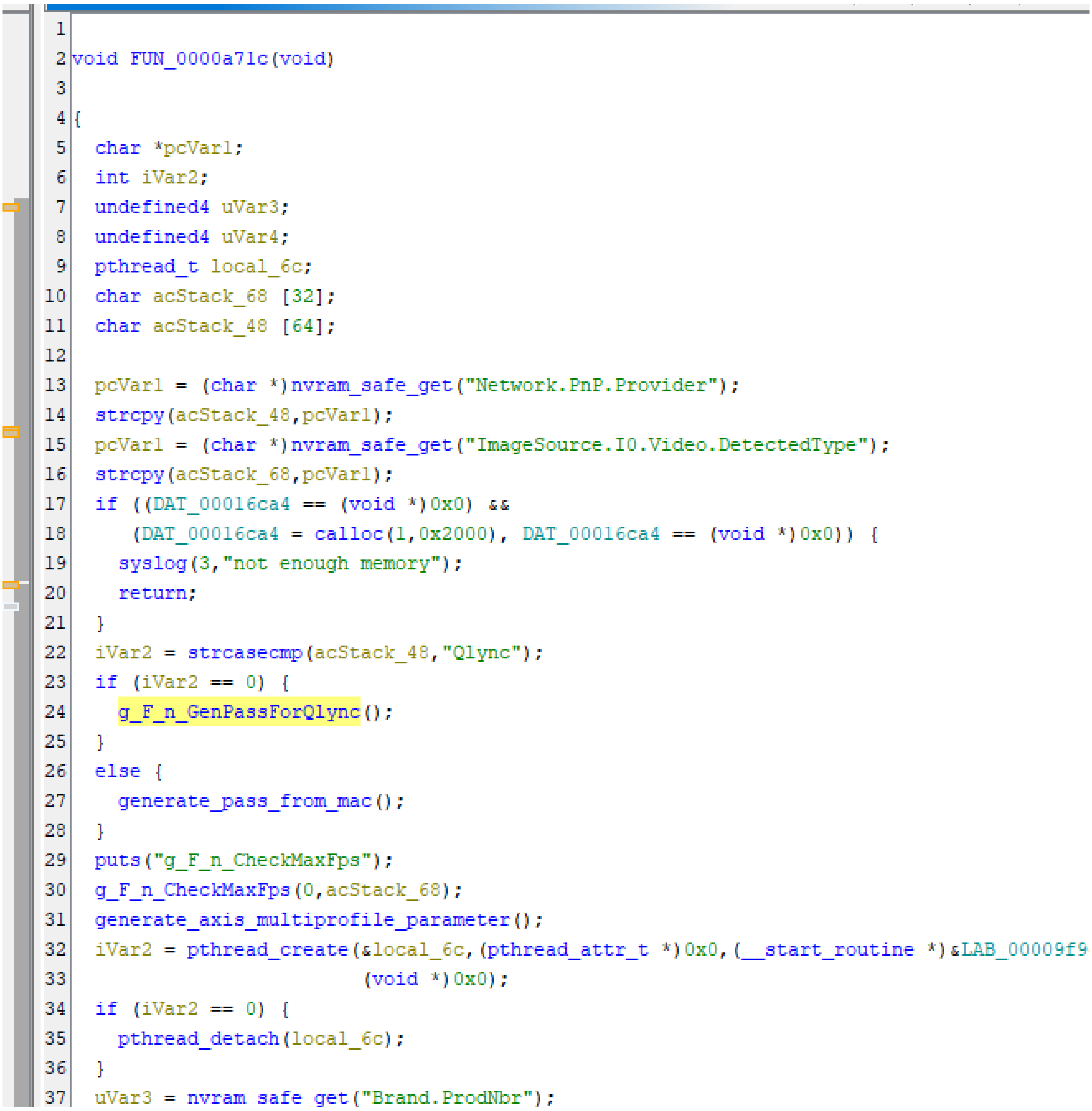
description

In D-link-ipcamera DCS-7517B1 firmware, binary `/bin/httpd` contains a hardcoded weak password vulnerability. When the device detects that the provider is "Qlync", a hardcoded root-level user account is created using a static password hashed from a known string.

This behavior allows an attacker to gain full administrative access using a fixed, publicly reversible password.

details

Within the `/bin/httpd` binary, the following logic determines which password initialization method is used:



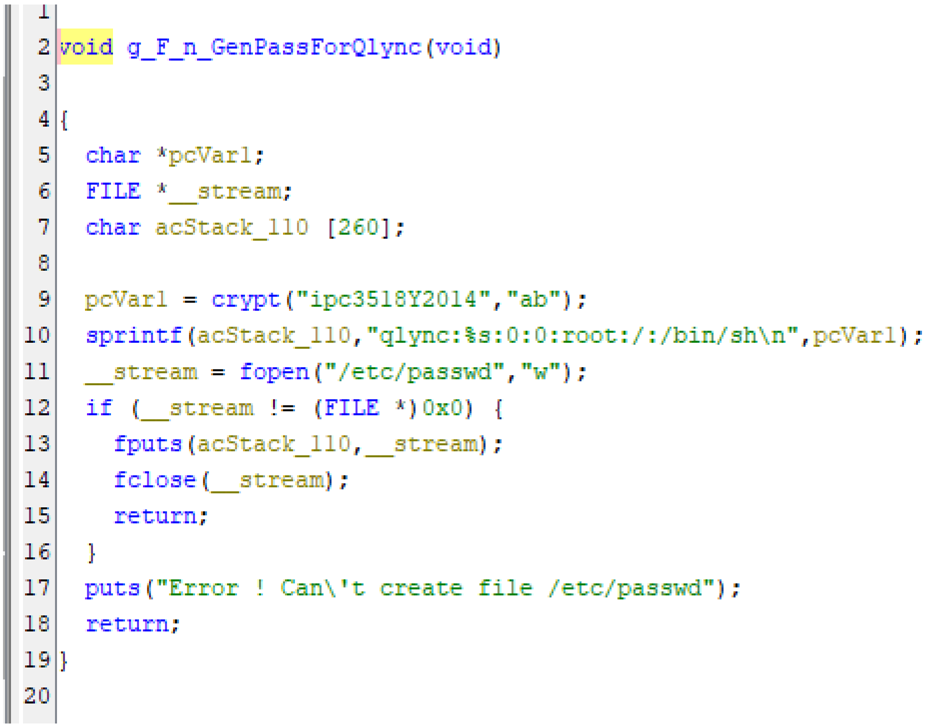
```

void FUN_0000a71c(void)

{
  char *pcVar1;
  int iVar2;
  undefined4 uVar3;
  undefined4 uVar4;
  pthread_t local_6c;
  char acStack_68 [32];
  char acStack_48 [64];

  pcVar1 = (char *)nvram_safe_get("Network.PnP.Provider");
  strcpy(acStack_48,pcVar1);
  pcVar1 = (char *)nvram_safe_get("ImageSource.I0.Video.DetectedType");
  strcpy(acStack_68,pcVar1);
  if ((DAT_00016ca4 == (void *)0x0) &&
     (DAT_00016ca4 = calloc(1,0x2000), DAT_00016ca4 == (void *)0x0)) {
    syslog(3,"not enough memory");
    return;
  }
  iVar2 = strcasecmp(acStack_48,"Qlync");
  if (iVar2 == 0) {
    g_F_n_GenPassForQlync();
  }
  else {
    generate_pass_from_mac();
  }
  puts("g_F_n_CheckMaxFps");
  g_F_n_CheckMaxFps(0,acStack_68);
  generate_axis_multiprofile_parameter();
  iVar2 = pthread_create(&local_6c,(pthread_attr_t *)0x0,(__start_routine *)&LAB_00009f9
                         (void *)0x0);
  if (iVar2 == 0) {
    pthread_detach(local_6c);
  }
  uVar3 = nvram_safe_get("Brand.ProdNbr");
```

If the NVRAM key Network.PnP.Provider is set to "Qlync", the system calls g_F_n_GenPassForQlync() to generate a static password.

The root password is generated from the static string "ipc3518Y2014" with a fixed salt "ab".

The hashed result is written into /etc/passwd as user qlync, who has UID=0, GID=0, granting superuser privileges.

Since both the password input and salt are hardcoded and publicly visible, the resulting password hash can be trivially replicated by an attacker.



```

void g_F_n_GenPassForQlync(void)

{
  char *pcVar1;
  FILE *__stream;
  char acStack_110 [260];

  pcVar1 = crypt("ipc3518Y2014","ab");
  sprintf(acStack_110,"qlync:%s:0:0:root:/:/bin/sh\n",pcVar1);
  __stream = fopen("/etc/passwd","w");
  if (__stream != (FILE *)0x0) {
    fputs(acStack_110,__stream);
    fclose(__stream);
    return;
  }
  puts("Error ! Can\'t create file /etc/passwd");
  return;
}

```