DCS-6517B1_FW_v2.02.01 Weak Password Vulnerability

- vendor: dlink
- product: DCS-6517B1
- version: below or equal v2.02.01
- support url: https://www.dlink.com/uk/en/products/dcs-6517-5-megapixel-varifocal-outdoor-dome-network-camera
- firmware download url: https://files.dlink.com.au/products/DCS-6517/REV_B/Firmware/Firmware_2.02.01/

description

In D-link DCS-6517B1 firmware, binary `/bin/httpd` contains a hardcoded weak password vulnerability. A root-level user account is created using a static password.

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

details

In the affected firmware, the binary /bin/httpd calls the function generate_pass_from_mac from the libnvram.so shared library. This function programmatically generates user credentials based on the device's MAC address and writes them into the /etc/passwd file. Critically, it also injects a hardcoded root user entry:

```
root:abATsxpNxEp4Y:0:0:root:/:/bin/sh
```

```
  }
  else {
    strcpy(local_138,pcVar3);
  }
  printf("generate_pass_from_mac %s %s %s\n",acStack_14c,local_168,local_138);
  pcVar3 = crypt(local_138,"ab");
  nvram_set_no_modify_flag("user.username_from_mac",acStack_15c);
  nvram_set_no_modify_flag("user.password_from_mac",local_138);
  sprintf(acStack_118,"root:abATsxpNxEp4Y:0:0:root:/:/bin/sh\n%s:%s:0:0:root:/:/bin/sh\n",
          acStack_15c,pcVar3);
  __stream = fopen("/etc/passwd","w");
  if (__stream == (FILE *)0x0) {
    puts("Error ! Can\'t create file /etc/passwd");
    return;
  }
  fputs(acStack_118,__stream);
  fclose(__stream);
  return;
}
```

The password hash abATsxpNxEp4Y corresponds to a static, hardcoded password using the crypt() function with a known salt.

Special Note

I have already applied a CVE related to the same function, which addresses the predictable password generation from the MAC address. This report covers a separate vulnerability involving the hardcoded static root password written into /etc/passwd, and should be treated as a distinct issue.