

D-Link dir890L hardcoded login shell

Description

In D-Link dir890L devices, there contains a hard-coded credential for UART authentication. Users can log in into the device's UART port via the hard-coded credential and gain root privilege.

Affected devices: D-Link dir890L, Official URL: <https://www.dlink.com/uk/en/products/dir-890l-ac3200-ultra-wifi-router>

Affected Versions: Versions up to DIR890LA1_FW111b04.

Firmware download URL: https://files.dlink.com.au/products/DIR-890L/REV_A/Firmware/Firmware_v1.20b01/DIR890LA1_FW111b04.bin

Details

In the `rgbin` binary of D-Link dir890L, the authentication for UART is handled via function at address `0xD084`. It compares user's input with credential retrieved from system configuration, the system will use the hardcoded credential `35dHJLI!wyX:ut77a3d33w` for authentication with the configuration in case UART is enabled.

```
19  if ( !strcmp(s1a, "login") )
20  return sub_D084(a1, (int)a2);

38      case 'c':
39          get_sys_config(0, 0, "/sys/user:1/name", uname, 79);
40          get_sys_config(0, 0, "/sys/user:1/password", pwd, 79);
41          v14 = 1;
42          continue;
43      case 'l':
44          off_2D340[0] = (char *)optarg;
45          continue;
46      case 't':
47          dword_2D33C = atoi((const char *)optarg);
48          if ( dword_2D33C < 0 )
49              dword_2D33C = 60;
50          continue;
51      case 'u':
52          strncpy(uname, "35dHJLI!wyX", 0x50u);
53          strncpy(pwd, "ut77a3d33w", 0x50u);
54          continue;
55      default:
56          goto LABEL_2;
57      }
58  }
59  break;
60  }
61  }
62  if ( access(off_2D340[0], 1) >= 0 )
63  {
64      signal(14, (__sig_handler_t)sub_CA68);
65      alarm(dword_2D33C);
66      while ( v16 <= 2 && (s2[0] || sub_CAF0(s2, 80) >= 0) )
67      {
68          if ( !strcmp(uname, s2) )
69          {
70              sub_CD0C(v9, 80);
71              if ( !strcmp(pwd, v9) || !pwd[0] && strlen(v9) == 1 && v9[0] == 10 )
72              {
73                  alarm(0);
74                  system(off_2D340[0]);
75                  return 0;
76              }
77          }
78          sleep(3u);
79          printf("Login incorrect");
80          s2[0] = 0;
```

The security impact would be a attacker having physical access to the device and uses UART to login into the device and gain root privilege.