

master



Vulns_of_Embedded_Systems / Two stack overflows were found in DIR-615Jx10.0 Devices.pdf



ladinas Add files via upload ...

History

1 contributor

141 KB



Two stack overflows were found in DIR-615Jx10 Devices

@ladinas, @chandlerchen, @bitpeach

Affected versions:

All firmware versions of D-Link DIR-615Jx10

Vulnerabilities Analysis:

Download the GPL source code and the firmbin from D-Link official websites. Open the source file “/boa/src/fmwlan.c” since the HTTP service is implemented by boa in these devices. As we can see in the function “formWlanSetup”, value of the parameter “webpage” is copied to the variable “buffer” without any string length checking, which causes the stack overflow. The same analysis can be done in the function “formWlanSetup_Wizard”.

```
void formWlanSetup(request *wp, char *path, char *query)
{
    char tmpBuf[100];
    int settingsChanged=0, need_reinit=0, wps_disabled, wps_config, is_from_wizard;
    char *strValue;
    int oriWlanMode;
    char buffer[200];
    char *CurTime;
    CurTime = (char *)websGetVar(wp, T("curTime"), "");

    int ssid_modify = 0;
    char *strVal;
#ifdef DAP1332_MX
    strVal = (char *)websGetVar(wp, T("f_ssid_status"), T(""));
    ssid_modify = atoi(strVal);
#endif
    strValue= (char *)websGetVar(wp, T("webpage"), T(""));
    strcpy(last_url, strValue);

    strValue= websGetVar(wp, T("settingsChanged"), T(""));
    if (strValue[0])
        settingsChanged = atoi(strValue);

    apmib_get(MIB_WSC_CONFIGURED, (void *)&wps_config);
    apmib_get(MIB_WSC_DISABLE, (void *)&wps_disabled);
    apmib_get(MIB_WLAN_MODE, (void *)&oriWlanMode);

    if(settingsChanged == 1)
    {
        if (wlanHandler(wp, tmpBuf, &need_reinit, &is_from_wizard) < 0)
        {
            strcpy(err_msg, tmpBuf);
            sprintf(buffer, "%s", last_url);
        }
    }
}
```



