

bug1

## Basic Information

Download link

<https://www.dlinktw.com.tw/techsupport/download.ashx?file=3458>

vulnerability file

cgibin

function address

40EDA4

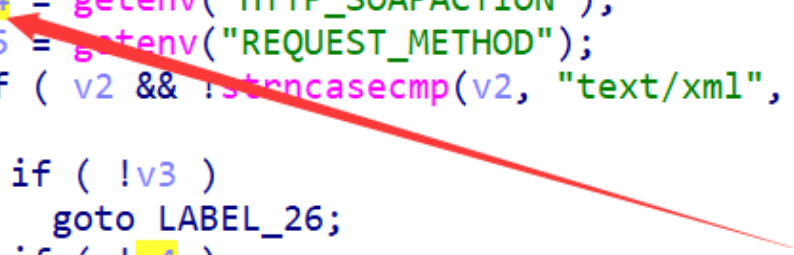
Vulnerability type

stack overflow

## Details

The HTTP\_SOAPACTION parameter can be entered by the user and passed to the dword\_428330 parameter. The sub\_40eda4 function is then called, using the dword\_428330 parameter, and copied to the stack with a space of 260 bytes, causing a stack overflow.

```
v2 = getenv("CONTENT_TYPE");
v3 = getenv("REQUEST_URI");
v4 = getenv("HTTP_SOAPACTION");
v5 = getenv("REQUEST_METHOD");
if ( v2 && !strncasecmp(v2, "text/xml", 8u) )
{
    if ( !v3 )
        goto LABEL_26;
    if ( !v4 )
```



```

v14 = &v4[strlen(v4) - 1];
if ( *v14 == 34 )
    *v14 = 0;
v15 = &v4[*v4 == 0x22];
v16 = strchr(v15, '#');
dword_438330 = (int)v16;
if ( !v16 )
{

```

```

void __fastcall sub_40EDA4(int a1, _DWORD *a2)
{
    const char *string; // $v0
    int v4; // $v0
    _DWORD *parameter_nodehead; // $s1
    char v6[260]; // [sp+18h] [-104h] BYREF

    memset(v6, 0, 0x100u);
    if ( *a2 == 2 )
    {
        string = sobj_get_string(a2[1]);
        v4 = ixmlParseBuffer(string);
        if ( v4 )
        {
            parameter_nodehead = (_DWORD *)get_parameter_nodehead(v4);
            if ( parameter_nodehead )
            {
                sprintf(v6, "%s action_name", byte_436EF0);
                xmldb_set(0, 0, v6, dword_438330);
                sprintf(v6, "%s/%s", byte_436EF0, (const char *)dword_438330);
                if ( parameter_nodehead[8] )
                    sub_40EC5C(v6);
                free(parameter_nodehead);
            }
        }
    }
}

```

Author

archer@TalentSec Co.,Ltd