

1G - Bug #3481

ssdpd dnsproxy

05/15/2025 09:47 -

Status:	Closed	Start date:	05/15/2025
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:		Spent time:	0.00 hour
:	emei_V1.0.2_ker_fs_53f245d4.bin	:	100%

Description

1. shell netstat -nutap|grep -v '127.0.0.1'

2. ps |grep pid

3. cat/etc/passwd|grep "Linux"uidgiduidgid":34

4. cat /proc/pid/status |grep CapEff

5. Linux PC capsh

vsftpdssdpdnsproxycap_chowncap_dac_overridecap_dac_read_searchcap_fownercap_setgidcap_setuidcap_sys_module

1. 4IDuidIDgido

2. 1

cap_chowncap_dac_overridecap_dac_read_searchcap_fownercap_setgidcap_setuidcap_sys_module

1. netstat -nutap|grep -v '127.0.0.1'

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	18.18.46.26:46000	0.0.0.0:*	LISTEN	1505/hi_appm
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	4603/uhttpd
tcp	0	0	0.0.0.0:8080	0.0.0.0:*	LISTEN	1542/webServer
tcp	0	0	0.0.0.0:53	0.0.0.0:*	LISTEN	25539/dnsmasq
tcp	0	0	0.0.0.0:5431	0.0.0.0:*	LISTEN	4180/miniupnpd
tcp	0	0	192.168.1.1:23	0.0.0.0:*	LISTEN	3820/telnetd
tcp	0	0	192.168.1.1:17998	0.0.0.0:*	LISTEN	4502/cloudclocal
tcp	0	0	192.168.1.1:80	192.168.1.123:4123	TIME_WAIT	-
tcp	0	0	10.10.100.191:50766	218.78.34.61:6880	ESTABLISHED	4501/cloudclient
tcp	0	55	192.168.1.1:23	192.168.1.123:3634	ESTABLISHED	3820/telnetd
tcp	0	0	192.168.1.1:8080	192.168.1.123:4122	TIME_WAIT	-
tcp	0	0	192.168.1.1:80	192.168.1.123:4124	ESTABLISHED	4603/uhttpd
tcp	0	0	:::80	:::*	LISTEN	4603/uhttpd
tcp	0	0	fe80::1:8080	:::*	LISTEN	1542/webServer
tcp	0	0	:::53	:::*	LISTEN	25539/dnsmasq
tcp	0	0	fe80::1:23	:::*	LISTEN	3831/telnetd
udp	0	0	18.18.102.84:5060	0.0.0.0:*		4839/sipapp
udp	0	0	192.168.1.1:5351	0.0.0.0:*		4180/miniupnpd
udp	0	0	0.0.0.0:32768	0.0.0.0:*		4511/ssdpd
udp	0	0	192.168.1.1:44802	0.0.0.0:*		4180/miniupnpd
udp	0	0	10.0.3.1:53000	0.0.0.0:*		4433/dnsproxy
udp	0	0	0.0.0.0:53	0.0.0.0:*		25539/dnsmasq
udp	0	0	0.0.0.0:67	0.0.0.0:*		25539/dnsmasq
udp	0	0	0.0.0.0:1900	0.0.0.0:*		4180/miniupnpd
udp	0	0	:::546	:::*		3987/odhcp6c
udp	0	0	:::546	:::*		3437/odhcp6c
udp	0	0	:::546	:::*		3191/odhcp6c
udp	0	0	:::547	:::*		25539/dnsmasq
udp	0	0	:::53	:::*		25539/dnsmasq

3. ps |grep 1505

1505 network 14:15 {cwmp} hi_appm -v 6 -i /config/conf/appm/init -c /config/conf/appm/xml/gpon.xml

3604 root 0:00 grep 1505

```

4. ps |grep 4603
   3620 root    0:00 grep 4603
   4603 network 0:00 /usr/sbin/uhttpd -f -h /www -r SAF -x /cgi-bin -t 60 -T 30 -k 20 -A 1 -n 3 -N 100 -R -p 0.0.0.0:80 -p [::]:80
5. ps |grep 1542
   1542 network 0:00 webServer
   3625 root    0:00 grep 1542
6. ps |grep 25539
   3630 root    0:00 grep 25539
   25539 network 0:18 dnsmasq -C /tmp/etc/dnsmasq.conf -c 0 --all-servers
7. ps |grep 4180
   3634 root    0:00 grep 4180
   4180 hsan    0:03 /usr/sbin/miniupnpd -f /tmp/miniupnpd.conf -i wan4_101
8. ps |grep 3820
   3639 root    0:00 grep 3820
   3820 network 0:00 telnetd -t -b 192.168.1.1 -p 23 -l /bin/login
9. ps |grep 4502/
   3644 root    0:00 grep 4502/
10. ps |grep 4502
   3646 root    0:00 grep 4502
   4502 hsan    0:00 /sbin/cloudclocal
11. ps |grep 4501
   3653 root    0:00 grep 4501
   4501 hsan    0:04 /sbin/cloudclient
12. ps |grep 3820
   3659 root    0:00 grep 3820
   3820 network 0:00 telnetd -t -b 192.168.1.1 -p 23 -l /bin/login
13. ps |grep 3831
   3669 root    0:00 grep 3831
   3831 network 0:00 telnetd -t -b fe80::1%br0 -p 23 -l /bin/login
14. ps |grep 4839
   3673 root    0:00 grep 4839
   4839 network 40:06 /usr/bin/sipapp
15. ps |grep 4511
   3678 root    0:00 grep 4511
   4511 root    0:00 /sbin/ssdpd
16. ps |grep 4433
   3683 root    0:00 grep 4433
   4433 root    0:02 /usr/bin/dnspoxy
17. ps |grep 3987
   3695 root    0:00 grep 3987
   3987 hsan    0:15 odhcp6c -s /usr/wan_proto/dhcpv6.script -N try -P 0 -t 120 pppoe-wan2_100
18. ps |grep 3437
   3437 hsan    0:15 odhcp6c -s /usr/wan_proto/dhcpv6.script -N try -P 0 -t 120 wan4_101
   3701 root    0:00 grep 3437
19. ps |grep 3191
   3191 hsan    0:15 odhcp6c -s /usr/wan_proto/dhcpv6.script -N try -P 0 -t 120 wan3_102
   3706 root    0:00 grep 3191 #

```

```

1. cat /etc/passwd
root:x:0:0:root:/root:/bin/ash
hsan:x:1000:1000:Linux User,,,:/root:/bin/ash
network:x:1001:1000:Linux User,,,:/mnt:/bin/ash
nobody:*:65534:65534:nobody:/var:/bin/false
telnetadmin_telnet:x:1002:1000:Linux User,,,:/root:/bin/ash

```

```
cat /proc/3191/status |grep CapEff
```

```

1. cat /proc/1505/status |grep CapEff
CapEff: 000000001000b400
2. cat /proc/4603/status |grep CapEff
CapEff: 0000000000000000
3. cat /proc/1542/status |grep CapEff
CapEff: 000000001000b400
4. cat /proc/25539/status |grep CapEff
CapEff: 000000001000b400
5. cat /proc/4180/status |grep CapEff
CapEff: 000000fffffeff30

```

```
6. cat /proc/3820/status |grep CapEff
CapEff: 000000001000b400
7. cat /proc/4502/status |grep CapEff
CapEff: 0000000000000000
8. cat /proc/4501/status |grep CapEff
CapEff: 0000000000000000
9. cat /proc/3820/status |grep CapEff
CapEff: 000000001000b400
10. cat /proc/3831/status |grep CapEff
CapEff: 000000001000b400
11. cat /proc/4839/status |grep CapEff
CapEff: 000000ffffeff30
12. cat /proc/4511/status |grep CapEff
CapEff: 000001ffffffff
13. cat /proc/4433/status |grep CapEff
CapEff: 000001ffffffff
14. 3987
ash: 3987: not found
15. cat /proc/3987/status |grep CapEff
CapEff: 000000ffffeff30
16. cat /proc/3437/status |grep CapEff
CapEff: 000000ffffeff30
17. cat /proc/3191/status |grep CapEff
CapEff: 000000ffffeff30 #

capsh --decode=000001ffffffff

0x000000001000b400=cap_net_bind_service,cap_net_admin,cap_net_raw,cap_ipc_owner,cap_lease

0x0000000000000000=

0x000000ffffeff30=cap_fsetid,cap_kill,cap_setpcap,cap_linux_immutable,cap_net_bind_service,cap_net_broadcast,cap_net_admin,
cap_net_raw,cap_ipc_lock,cap_ipc_owner,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_
boot,cap_sys_nice,cap_sys_resource,cap_sys_time,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,c
ap_setfcap,cap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend,37,38,39

0x000001ffffffff=cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_se
tpcap,cap_linux_immutable,cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc_owner,cap
_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_
_resource,cap_sys_time,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,cap_setfcap,cap_mac_overri
de,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend,37,38,39,40

cap_chown[]cap_dac_override[]cap_dac_read_search[]cap_fowner[]cap_setgid[]cap_setuid[]cap_sys_module
```

History

#1 - 05/19/2025 10:00 - 

- Status changed from New to Feedback

- Assignee changed from  to 

ssdpddnsproxy

#2 - 05/20/2025 10:20 - 

- Status changed from Feedback to Closed

ssdpddnsproxyemei_default_ker_fs_fw_819f8a64.bin