

EETI Android SELinux Config Guide

Reference for Android Q

Base on RK3399

TABLE OF CONTENTS

TABLE OF CONTENTS.....	0
SELinux Permission Setting.	1

All information provided in this document is for reference only and is tested on RK3399 Android Q. User shall modify the contents based on the operating system and its environment.

SELinux Permission Setting.

1. Bind file for eGTouchD Service:

Add the string in to below files:

"YourAndroid/system/sepolicy/prebuilts/api/26.0/private/file_contexts"

"YourAndroid/system/sepolicy/prebuilts/api/27.0/private/file_contexts"

"YourAndroid/system/sepolicy/prebuilts/api/28.0/private/file_contexts"

"YourAndroid/system/sepolicy/prebuilts/api/29.0/private/file_contexts"

"YourAndroid/system/sepolicy/private/file_contexts"

```
#EETI
/system/bin/eGTouchD      u:object_r:eGTouchD_exec:s0
/data/eGalax(/.*)?        u:object_r:eGalax_data_file:s0
```

2. Modified 26.0.cil file

Add the string in to below 26.0.cil files:

"YourAndroid/system/sepolicy/prebuilts/api/27.0/private/compat/26.0/26.0.cil"

"YourAndroid/system/sepolicy/prebuilts/api/28.0/private/compat/26.0/26.0.cil"

"YourAndroid/system/sepolicy/prebuilts/api/29.0/private/compat/26.0/26.0.cil"

"YourAndroid/system/sepolicy/private/compat/26.0/26.0.cil"

```
(typeattributeset eGTouchD_26_0 (eGTouchD))
(typeattributeset eGTouchD_exec_26_0 (eGTouchD_exec))
```

3. Modified 27.0.cil file

Add the string in to below 27.0.cil files:

"YourAndroid/system/sepolicy/prebuilts/api/28.0/private/compat/27.0/27.0.cil"

"YourAndroid/system/sepolicy/prebuilts/api/29.0/private/compat/27.0/27.0.cil"

"YourAndroid/system/sepolicy/private/compat/27.0/27.0.cil"

```
(expandtypeattribute (eGTouchD_27_0) true)
(expandtypeattribute (eGTouchD_exec_27_0) true)
(typeattributeset eGTouchD_27_0 (eGTouchD))
(typeattributeset eGTouchD_exec_27_0 (eGTouchD_exec))
```

4. Modified nonplat_sepolicy.cil file

Add the string in to below nonplat_sepolicy.cil files:

"YourAndroid/system/sepolicy/prebuilts/api/26.0/nonplat_sepolicy.cil

```
(typeattributeset domain (eGTouchD_26_0 adbd_26_0 audioserver_26_0 blkid_26_0 blkid_untrusted_26_0 .....
(typeattributeset file_type (eGTouchD_exec_26_0 bootanim_exec_26_0 bootstat_exec_26_0 bufferhubd_exec_26_0...
(typeattributeset exec_type (eGTouchD_exec_26_0 bootanim_exec_26_0 bootstat_exec_26_0 bufferhubd_exec_26_0
(typeattribute eGTouchD_26_0)
(roletype object_r eGTouchD_26_0)
(typeattribute eGTouchD_exec_26_0)
(roletype object_r eGTouchD_exec_26_0)
```

5. Modified nonplat_sepolicy.cil file

Add the string in to below nonplat_sepolicy.cil files:

"YourAndroid/system/sepolicy/prebuilts/api/27.0/nonplat_sepolicy.cil

```
(typeattributeset domain (eGTouchD_27_0 adbd_27_0 audioserver_27_0 blkid_27_0 blkid_untrusted_27_0 .....
(typeattributeset file_type (eGTouchD_exec_27_0 bootanim_exec_27_0 bootstat_exec_27_0 bufferhubd_exec_27_0...
(typeattributeset exec_type (eGTouchD_exec_27_0 bootanim_exec_27_0 bootstat_exec_27_0 bufferhubd_exec_27_0
(typeattribute eGTouchD_27_0)
(roletype object_r eGTouchD_27_0)
(typeattribute eGTouchD_exec_27_0)
(roletype object_r eGTouchD_exec_27_0)
```

6. Add eGTouchD permission:

Add the below new files:

"Android/system/sepolicy/prebuilts/api/26.0/private/eGTouchD.te"

"Android/system/sepolicy/prebuilts/api/27.0/private/eGTouchD.te"

"Android/system/sepolicy/prebuilts/api/28.0/private/eGTouchD.te"

"Android/system/sepolicy/prebuilts/api/29.0/private/eGTouchD.te"

"Android/system/sepolicy/private/eGTouchD.te"

```
typeattribute eGTouchD coredomain;
```

```
init_daemon_domain(eGTouchD)
```

7. Add eGTouchD permission:

Add the below new files:

“Android/system/sepolicy/prebuilts/api/26.0/public/eGTouchD.te”

“Android/system/sepolicy/prebuilts/api/27.0/public/eGTouchD.te”

“Android/system/sepolicy/prebuilts/api/28.0/public/eGTouchD.te”

```
type eGTouchD, domain;

type eGTouchD_exec, exec_type, file_type, system_file_type;

type eGalax_data_file, file_type, data_file_type, core_data_file_type, mltrustedobject;

set_prop(eGTouchD, system_prop)
```

8. Add eGTouchD permission:

Add the below new files:

“Android/system/sepolicy/prebuilts/api/29.0/public/eGTouchD.te”

“Android/system/sepolicy/public/eGTouchD.te”

Depending on the system, user may need to add your own rules

```
type eGTouchD, domain;

type eGTouchD_exec, exec_type, file_type, system_file_type;

type eGalax_data_file, file_type, data_file_type, core_data_file_type, mltrustedobject;

set_prop(eGTouchD, system_prop)

allow eGTouchD shell_exec:file { read open execute execute_no_trans getattr map };
allow eGTouchD system_data_file:dir { write read open add_name remove_name setattr getattr create search };
allow eGTouchD system_data_file:file { read open ioctl write unlink getattr setattr create unlink append };
allow eGTouchD system_data_file:fifo_file { read open ioctl write unlink getattr setattr create };
allow eGTouchD eGalax_data_file:dir { write read open add_name remove_name setattr getattr create search };
allow eGTouchD eGalax_data_file:file { read open ioctl write unlink getattr setattr create unlink append };
allow eGTouchD eGalax_data_file:fifo_file { read open ioctl write unlink getattr setattr create };
allow eGTouchD toolbox_exec:file { read open execute execute_no_trans getattr map };
allow eGTouchD proc:file { write read open getattr };
allow eGTouchD sysfs:dir { read open search };
allow eGTouchD sysfs:file { write read open getattr };
allow eGTouchD device:chr_file { open read write ioctl getattr };
allow eGTouchD device:dir { open read write ioctl getattr };
allow eGTouchD uhid_device:chr_file { open read write ioctl getattr };
allow eGTouchD input_device:dir { open read search };
allow eGTouchD input_device:chr_file { getattr setattr };
```

```
allow eGTouchD eGTouchD:capability { sys_boot dac_override dac_read_search fowner fsetid };
allow eGTouchD system_file:file { read open execute execute_no_trans getattr };
allow eGTouchD eGTouchD:capability { kill };
allow eGTouchD properties_device:dir { read open map };
allow eGTouchD properties_device:file { read open map };
allow eGTouchD proc_stat:file { read open getattr };
allow eGTouchD proc_version:file { write read open getattr };
allow eGTouchD serial_device:chr_file { write read open getattr ioctl };
allow eGTouchD proc_modules:file { write read open getattr };
allow eGTouchD system_data_file:fifo_file { read open ioctl write unlink getattr setattr create };

####For EETI APK TOOL####
allow untrusted_app eGalax_data_file:fifo_file { open read write };
allow untrusted_app eGalax_data_file:dir { open read write search };
allow untrusted_app_27 eGalax_data_file:fifo_file { open read write };
allow untrusted_app_27 eGalax_data_file:dir { open read write search };
```

8. Add Exceptions permission rules:

After adding these permissions, errors may occur during compilation.

This may be due to the conflict between some neverallow rules such as eGTouchD.te and other .te files.

Depending on the system, user may need to add some exceptions to the rules.

Add the string to the file below in red:

“YourAndroid/system/sepolicy/private/coredomain.te” &

“YourAndroid/system/sepolicy/prebuilts/api/29.0/private/coredomain.te”

```
neverallow {
    coredomain
    -init
    -vold
    -eGTouchD
} proc:file no_rw_file_perms;
```

```
neverallow {
    coredomain
    -init
    -ueventd
    -vold
    -eGTouchD
} sysfs:file no_rw_file_perms;
```

Add the string to the file below in red:

"YourAndroid/system/sepolicy/private/domain.te" &

"YourAndroid/system/sepolicy/prebuilts/api/29.0/private/domain.te"

```
vendor_init
vold
vold_prepare_subdirs
zygote
eGTouchD
}')
neverallow ~dac_override_allowed self:global_capability_class_set dac_override;
```

Add the string to the file below in red:

"YourAndroid/system/sepolicy/public/domain.te" &

"YourAndroid/system/sepolicy/prebuilts/api/29.0/public/domain.te"

```
neverallow { domain -eGTouchD } device:chr_file { open read write };
```

```
neverallow {
    domain
    -coredomain
    -appdomain
    -vendor_executes_system_violators
    -eGTouchD
    -vendor_init
} {
    system_file_type
```

```
-vold_prepare_subdirs # For unlink
-eGTouchD
with_asan(`-asan_extract')
} system_data_file:file no_w_file_perms;
```