

Donnerstag, 13. März 2008

## FreeBSD: X in der Jail

Alexander Leidinger hat für FreeBSD 7.0 (RELENG\_7(\_0)) und HEAD einen Patch bereitgestellt, welcher es ermöglicht X in einer Jail auszuführen. Durch den Patch ist es möglich auf /dev/io zuzugreifen welches der X Server braucht um in einer Jail zu funktionieren. Module welche normalerweise der X Server lädt, müssen zuvor manuell, oder über den loader geladen werden.

Alexander Leidinger, welcher eine Radeon Karte nutzt, hat hier

```
radeon_load="YES"
```

in die loader.conf eingetragen.

Der X Server sollte auch ohne dies funktionieren, allerdings würde die Beschleunigung (acceleration) fehlen.

Auch muss, neben dem Patch, noch /etc/devfs.rules geändert werden. Hier hat Alexander Leidinger seine devfs.rules gepostet (diese enthält einiges mehr als für den X-Server gebraucht wird):

```
[devfsrules_unhide_audio=5]
add path 'audio*' unhide
add path 'dsp*' unhide
add path 'midistat' unhide
add path 'mixer*' unhide
add path 'music*' unhide
add path 'sequencer*' unhide
add path 'sndstat' unhide
add path 'speaker' unhide
```

```
[devfsrules_unhide_printers=6]
add path 'lpt*' unhide
add path 'ulpt*' unhide
add path 'unlpt*' unhide
```

```
[devfsrules_unhide_input=7]
add path 'atkbd*' unhide
add path 'kbd*' unhide
add path 'joy*' unhide
add path 'psm*' unhide
add path 'sysmouse' unhide
add path 'ukbd*' unhide
add path 'ums*' unhide
```

```
[devfsrules_unhide_xorg=8]
add path 'agpgart' unhide
#add path 'console' unhide
add path 'dri' unhide
add path 'dri*' unhide
add path 'io' unhide
add path 'mem' unhide
#add path 'pci' unhide
add path 'tty' unhide
add path 'ttyv0' unhide
add path 'ttyv1' unhide
add path 'ttyv8' unhide
```

```
[devfsrules_unhide_cam=9]
```

```
add path 'da*' unhide
add path 'cd*' unhide
```

```
[devfsrules_unhide_kmem=10]
add path kmem unhide
```

```
#
# This allows to run a desktop system in a jail. Think about what you want to
# achieve before you use this, it opens up the entire machine to access from
# this jail to any sophisticated program.
```

```
#
[devfsrules_jail_desktop=11]
add include $devfsrules_hide_all
add include $devfsrules_unhide_basic
add include $devfsrules_unhide_login
add include $devfsrules_unhide_audio
add include $devfsrules_unhide_input
add include $devfsrules_unhide_xorg
add include $devfsrules_unhide_cam
add include $devfsrules_unhide_kmem
```

Auch müssen die Regeln noch in der Jail angewandt werden:

```
jail__devfs_ruleset="devfsrules_jail_desktop"
```

Wie Alexander Leidinger schreibt hat er auch noch eine sysctl entsprechend gesetzt:

```
security.jail.dev_io_access_allowed=1
```

Noch relativ neu ist die man-page und die sysctl:

```
security.jail.dev_io_access_allowed_hostname
```

Alexander Leidinger hofft das er einiges an feedback bekommt.

Der Original-Post von Alexander Leidinger gibt es hier nachzulesen.

So werden die Jails mehr und mehr zu einem vollständigen System welches immer weniger Einschränkungen kennt. Dabei bleibt allerdings immer die Frage im Raum, wie sicher sind die Jails dann noch, oder werden hier noch unbekannte Sicherheitslücken aufgerissen.

Geschrieben von asg in FreeBSD um 08:36