



Mise à jour du module de sécurité SELinux pour le logiciel courier-imap

| | |
|--|----|
| <i>Mise à jour du module de sécurité SELinux pour le logiciel courier-imap</i> | 1 |
| Environnement d'exécution SELinux..... | 1 |
| Informations SELinux..... | 1 |
| Informations Gentoo..... | 1 |
| Validation des modifications des modules SELinux pour courier-imap..... | 1 |
| Correction initiale - relabellisation des fichiers du système..... | 2 |
| Chcon..... | 2 |
| semanage..... | 3 |
| Modification (minimale) de la politique courier..... | 4 |
| Modification de l'ebuild selinux-couier-imap..... | 4 |
| Validation des modifications..... | 4 |
| Patch externe – module fixCourier..... | 4 |
| Principaux aspects..... | 4 |
| Patches pour la version IMAP..... | 5 |
| Patches pour la version POP3..... | 7 |
| Version complète du fichier courier.te..... | 10 |

Il est à noter que ce travail a été effectué en partie lors d'un stage (été 2007) réalisé à l'ENST Bretagne de Rennes, France, équipe SERES. Ce document est un donc plus un document pas a pas qu'un réel patch. Etant donné qu'il s'agit d'un draft, je n'assure pas les résultats, bien que cela fonctionne parfaitement dans ma situation (voir les conditions décrites ci-dessous).

Merci de noter qu'il s'agit de version draft, non approuvée par la communauté hardened-gentoo dans dans la version actuelle.

Environnement d'exécution SELinux

Informations SELinux

```
SELinux status:      enabled
SELinuxfs mount:    /selinux
Current mode:        permissive
Mode from config file:  permissive
Policy version:      21
Policy from config file:  strict
```

Informations Gentoo

```
Linux 2.6.20-hardened-r5
net-mail/courier-imap-4.0.6-r2, options berkdb gdbm ipv6 nls (selinux)
```

Validation des modifications des modules SELinux pour courier-imap

La validation des modifications s'est basée sur deux critères.

Premièrement, une partie des relabellisations des fichiers s'appuie sur la version existante, mais non adaptée à la version actuelle de courier-imap, du fichier `/etc/security/seLinux/file_context`.

Les autres relabellisations sont des dérivées logique de celles-ci.

Pour la validation des modifications d'autorisations, plusieurs tests ont été effectués.

Les transitions de domaines ont été analysés via le statut retourné par `ps -eZ | grep <nom>` (<nom> = courier, principalement). Les modifications des autorisations de type allow découlent des alertes fournies par SELinux lors de l'initialisation des processus, sans connexion explicite aux serveurs (partie « lancement des processus » des patches) et la connexion au service via un webmail configuré pour utilisé pop ou imap (partie « Exécution » des patches)

Après avoir apporté ces modifications, plus aucune erreur relative à courier-imap (version pop et imap) n'a été relevée. La version proposée sur ce rapport a été également testée en tant que patch (ie sans modification incrémentale) sur la version pop du serveur.

Correction initiale - relabellisation des fichiers du système

La première étape de la correction du module consiste à relabelliser les différents fichiers du systèmes, si nécessaire.

Dans ce cas, deux outils sont possibles : `chcon` et `semanage`. `Chcon` permet de modifier immédiatement les types des fichiers, sans avoir à modifier les configurations SELinux. Il est utilisé pour modifier les informations sur les fichiers de bases (principalement accédé en lecture) de courier-imap. `Semanage` permet de configurer les autres données (fichiers run et lib).

Chcon

Cette partie décrit les modifications apportées par la relabellisation de fichiers du système, en utilisant l'outil `chcon()`. Ces modifications ont été apportées en se basant sur le fichier `fcontext` file (avec les anciennes informations de *courier-imap*). Celles-ci sont listées en **bleu**.

```

/usr/lib(64)?/courier/courier-authlib/*
system_u:object_r:courier_authdaemon_exec_t
chcon -t courier_authdaemon_exec_t /usr/lib/courier/courier-authlib/*

/usr/lib/courier-imap/* system_u:object_r:courier_exec_t
chcon -t courier_exec_t /usr/lib/courier-imap/*
chcon -t bin_t /usr/lib/courier-imap/

/usr/bin/imapd -- system_u:object_r:courier_pop_exec_t
chcon -t courier_pop_exec_t /usr/sbin/courier-imapd
chcon -t courier_pop_exec_t /usr/sbin/courier-pop3d

/usr/lib(64)?/courier/courier/imaplogin --
system_u:object_r:courier_pop_exec_t
chcon -t courier_pop_exec_t /usr/sbin/imaplogin

/usr/sbin/couriertcpd -- system_u:object_r:courier_tcpd_exec_t
chcon -t courier_tcpd_exec_t /usr/lib/courier-imap/couriertcpd

/usr/sbin/courierlogger -- system_u:object_r:courier_exec_t
chcon -t courier_exec_t /usr/sbin/courierlogger

```

```

chcon -ht courier_exec_t /usr/lib/courier-imap/courierlogger

chcon -t courier_var_run_t /var/run/imapd*
chcon -t courier_var_run_t /var/run/pop3*
chcon -t courier_var_run_t /var/run/authdaemon*

chcon -t courier_var_lib_t /var/lib/courier/authdaemon/
chcon -t courier_var_lib_t /var/lib/courier/authdaemon/*
chcon -t courier_var_lib_t /var/lib/courier/
chcon -t courier_var_lib_t /var/lib/courier-imap/couriersslcache

```

semanage

```

semanage fcontext -a -s system_u -t courier_var_run_t '/var/run/imapd.*'
semanage fcontext -a -s system_u -t courier_var_run_t '/var/run/pop3.*'
semanage fcontext -a -s system_u -t courier_var_run_t '/var/run/authdaemon?*'
semanage fcontext -a -s system_u -t courier_var_lib_t '/var/lib/courier'
semanage fcontext -a -s system_u -t courier_var_lib_t
'/var/lib/courier/authdaemon'
semanage fcontext -a -s system_u -t courier_var_lib_t
'/var/lib/courier/authdaemon/*'
semanage fcontext -a -t courier_var_lib_t '/var/lib/courier-
imap/couriersslcache'

```

Modification (minimale) de la politique courier

Après avoir modifier les labels des différents fichiers, il est également nécessaire de modifier les politiques définis dans le module courier pour SELinux.

Afin de limiter les problèmes au niveau du patch et de simplifier la gestion des modifications au niveau des différents serveurs, le choix suivant a été effectué : seule les modifications de base

devant obligatoirement être inscrite dans le fichier .te du module courier (ou autre module existant et géré par l'équipe gentoo) seront insérées dans le fichier du ebuild en question.

Les autres modifications sont apportées via un module externe, quickfixMvX, réduit ici à la partie courier-imap (nommée fixCourier dans ce document). Ces modifications externes sont indiquées dans la section suivante.

Modification de l'ebuild selinux-couier-imap

```
ebuild selinux-courier-imap-20070329.ebuild unpack
```

```
nano /var/tmp/portage/sec-policy/selinux-courier-imap-20070329/work/strict/courier.te
```

```
allow courier_authdaemon_t courier_tcpd_t:fifo_file rw_file_perms;  
+ files_pid_filetrans(courier_authdaemon_t,courier_var_run_t,file)  
corecmd_search_bin(courier_authdaemon_t)  
  
...  
# POP3/IMAP local policy  
#  
+ files_pid_filetrans(courier_tcpd_t,courier_var_run_t,file)  
allow courier_pop_t courier_authdaemon_t:tcp_socket
```

Validation des modifications

```
ebuild selinux-courier-imap-20070329.ebuild compile
```

```
ebuild selinux-courier-imap-20070329.ebuild install
```

```
ebuild selinux-courier-imap-20070329.ebuild qmerge
```

Une version complète du fichier « courier.te » est fournie en fin de rapport.

Patch externe – module fixCourier

Principaux aspects

Le patch externe a été élaboré en deux temps. La première partie définit les différentes autorisations pour assurer une bonne configuration de courier-imap lors du lancement du serveur.

Les modifications apportées concernent principalement

- un mauvais labelling des différents fichiers (paths ont changés)
- la configuration des transitions entre les processus (labelling des processus fils)
- la configuration des accès entre les différents composants de courier-imap

La deuxième partie des patches concerne la gestion de l'exécution des serveurs. Les différentes modifications sont donc liées à la collaboration entre les différentes fonctionnalités, notamment authdaemon & pop/imap. Des options pour les collaborations pop/imap & ldap et pop/imap & nfs sont également proposées.

Il est à noter que le patch est ici fourni en deux versions : IMAP et POP, dépendant du mode d'utilisation de courier-imap. Dans le cas d'une utilisation des deux modes sur le même serveur, il

est nécessaire de réunir les deux patches. Les différences entre ces patches sont indiqués dans les listings ci-dessous.

Cette différence entre les patches est probablement dû à la labellisation des processus fils : imap a le type `courier_pop_t` tandis que la version pop a le type `courier_tcpd_t`. Cette différence est minime mais engendre des patches différents.

Patches pour la version IMAP

```
module fixCourier 1.0;

require {
class capability { setgid setuid net_bind_service };
class chr_file { getattr read write };
class dir { add_name mounton remove_name write search getattr read
setattr};
class file { create execmod execute execute_no_trans getattr read unlink
write entrypoint ioctl lock link rename};
class lnk_file { create unlink read};
class netif udp_rcv;
class netlink_route_socket { bind create getattr nlmsg_read nlmsg_write
read write };
class node udp_rcv;
class sock_file { create rename setattr unlink write};
class tcp_socket { name_bind node_bind name_connect};
class udp_socket { name_bind node_bind rcv_msg };
class process { transition noatsecure rlimitinh siginh setrlimit};
class unix_stream_socket { listen };
class filesystem { associate };
class unix_stream_socket {connectto accept listen connect};

type bin_t;
type courier_authdaemon_t;
type courier_authdaemon_exec_t;
type courier_pop_t;

type courier_exec_t;
type courier_tcpd_t;
type courier_var_lib_t;
type device_t;
type fs_t;
type initrc_t;
type ldap_port_t;
type lib_t;
type nfs_t;
type node_t;
type pop_port_t;
type shell_exec_t;
type udev_t;
type user_home_dir_t;
type urandom_device_t;
type var_lib_t;
type var_run_t;
```

```
};

#
# // probleme POP - authdaemon
#
type_transition initrc_t courier_exec_t:process courier_tcpd_t;
allow courier_tcpd_t courier_exec_t:file entrypt;
allow courier_tcpd_t courier_exec_t:lnk_file read;
allow initrc_t courier_exec_t:file { execute read };

type_transition courier_tcpd_t courier_authdaemon_exec_t:process
courier_authdaemon_t;
allow courier_tcpd_t courier_authdaemon_t:process { noatsecure rlimitinh
siginh transition };
allow courier_tcpd_t courier_authdaemon_exec_t:file { execute read };

#
# les fichiers run de courier ont changés
# pas de répertoire distinct donc lecture possible sur var_lib_t
# pas de répertoire distinct donc lecture/ecriture possible sur
var_run_t:dir
allow courier_authdaemon_t var_lib_t:dir search;
allow courier_tcpd_t var_run_t:dir { add_name write };

allow courier_authdaemon_t courier_authdaemon_exec_t:dir { add_name
remove_name search write };
allow courier_authdaemon_t courier_authdaemon_exec_t:sock_file { create
rename setattr unlink };

#
# ?
allow courier_authdaemon_t self:unix_stream_socket listen;
allow courier_tcpd_t self:process setrlimit;

#
# Execution
#

allow courier_authdaemon_t courier_var_lib_t:dir { add_name remove_name
search write };
allow courier_authdaemon_t courier_var_lib_t:sock_file { create rename
setattr unlink };
allow courier_authdaemon_t self:netlink_route_socket { bind create
getattr nlmsg_read read write };
allow courier_authdaemon_t self:unix_stream_socket accept;

allow courier_tcpd_t courier_var_lib_t:sock_file write;
allow courier_pop_t courier_authdaemon_t:unix_stream_socket connectto;
allow courier_pop_t courier_exec_t:file { execute execute_no_trans
getattr ioctl read };
allow courier_pop_t courier_authdaemon_t:unix_stream_socket connect;
allow courier_pop_t urandom_device_t:chr_file { getattr read };
allow courier_pop_t var_lib_t:dir search;
```

```
allow courier_pop_t self:capability { setgid setuid };
allow courier_pop_t self:netlink_route_socket { bind create getattr
nlmsg_read read write };
allow courier_pop_t courier_var_lib_t:dir search;
allow courier_pop_t courier_var_lib_t:sock_file write;

#
# OPTIONS
#

#LDAP
allow courier_pop_t ldap_port_t:tcp_socket name_connect;

#Données sur NFS
# / ! \
# peut etre amélioré en spécifiant un type nfs_courier_t
allow courier_pop_t nfs_t:dir { add_name getattr read remove_name search
setattr write };
allow courier_pop_t nfs_t:file { create getattr link read unlink write };
allow courier_pop_t nfs_t:file rename;

# cette option pourrait peut être être améliorée
allow courier_pop_t shell_exec_t:file { execute read };
```

Patches pour la version POP3

```
module fixCourier 1.0;
```

```
require {
class capability {setgid setuid net_bind_service};
class chr_file { getattr read write };
class dir { add_name mounton read remove_name write search getattr };
class lnk_file { create unlink read};
class file { execute execute_no_trans getattr lock read write create
ioctl entypoint link unlink rename};
class netif udp_rcv;
class netlink_route_socket { bind create getattr nlmsg_read nlmsg_write
read write };
class node udp_rcv;
class sock_file { create getattr rename setattr unlink write };
class tcp_socket { name_bind node_bind name_connect};
class udp_socket { name_bind node_bind rcv_msg };
class process { transition noatsecure rlimitinh siginh };
class unix_stream_socket {connectto accept listen};

type courier_authdaemon_t;
type courier_authdaemon_exec_t;
type courier_exec_t;
type courier_pop_t;
type courier_tcpd_t;
type courier_var_lib_t;
type device_t;
```

```
type home_root_t;
type initrc_t;
type ldap_port_t;
type lib_t;
type nfs_t;
type node_t;
type pop_port_t;
type port_t;
type shell_exec_t;
type udev_t;
type user_home_dir_t;
type var_lib_t;
type var_run_t;
};

#
# // probleme POP - authdaemon

#
# CONFIGURATION : lancement des processus
#
type_transition initrc_t courier_exec_t:process courier_tcpd_t;
allow courier_tcpd_t courier_exec_t:file entrypoint;
allow courier_tcpd_t courier_exec_t:lnk_file read;
allow initrc_t courier_exec_t:file { execute read };

type_transition courier_tcpd_t courier_authdaemon_exec_t:process
courier_authdaemon_t;
allow courier_tcpd_t courier_authdaemon_t:process { noatsecure rlimitinh
siginh transition };
allow courier_tcpd_t courier_authdaemon_exec_t:file { execute read };

#
# les fichiers run de courier ont changes
# pas de repertoire distinct donc lecture possible sur var_lib_t
# pas de repertoire distinct donc lecture/ecriture possible sur
var_run_t:dir
allow courier_authdaemon_t var_lib_t:dir search;
allow courier_tcpd_t var_run_t:dir { add_name write };

allow courier_authdaemon_t courier_authdaemon_exec_t:dir { add_name
remove_name search write };
allow courier_authdaemon_t courier_authdaemon_exec_t:sock_file { create
rename setattr unlink };

#
# CONFIGURATION : Execution
#

allow courier_pop_t courier_exec_t:file execute;
allow courier_authdaemon_t courier_var_lib_t:dir { add_name remove_name
search write };
allow courier_authdaemon_t courier_var_lib_t:sock_file { create rename
```

```
setattr unlink };
allow courier_authdaemon_t self:netlink_route_socket { bind create
getattr nlmsg_read read write };
allow courier_authdaemon_t self:unix_stream_socket { accept listen };

allow courier_tcpd_t courier_authdaemon_t:unix_stream_socket connectto;

allow courier_tcpd_t self:capability { setgid setuid };
allow courier_tcpd_t self:netlink_route_socket { bind create getattr
nlmsg_read read write };
allow courier_tcpd_t courier_var_lib_t:sock_file write;
allow courier_tcpd_t home_root_t:dir search;
allow courier_tcpd_t courier_authdaemon_t:process signal;

#
# OPTIONS
#

# LDAP
allow courier_tcpd_t ldap_port_t:tcp_socket name_connect;

# Données sur NFS
# / ! \
# peut etre amélioré en spécifiant un type nfs_courier_t
allow courier_pop_t nfs_t:dir { getattr read search };
allow courier_pop_t nfs_t:file { getattr read };
allow courier_tcpd_t nfs_t:dir { getattr search };

# cette option pourrait peut être être améliorée
allow courier_tcpd_t shell_exec_t:file { execute read };
allow courier_pop_t nfs_t:dir { add_name remove_name write };
allow courier_pop_t nfs_t:file { create rename unlink write };
```