Distribution EOLE - Tâche #37560

Scénario # 37540 (Nouveau): AmonEcole 2.10 : tests clients Linux en erreur (problème cgroup ?)

etude

21/07/2026 11:25 - Ludwig Seys

Statut:	Fermé	**Début:**	21/07/2026
Priorité:	Normal	**Echéance:**	
Assigné à:	Ludwig Seys	**% réalisé:**	100%
Version cible:	Carnet Cadoles - MEN	**Temps estimé:**	0.00 heure

Description

Sur AmonEcole 2.10, la valeur kernel.yama.ptrace_scope=3, définie dans /etc/sysctl.conf, empêche LXCFS d'accéder aux informations du processus appelant nécessaires à la génération des fichiers virtualisés /proc/meminfo, /proc/cpuinfo et /proc/stat.

Ces fichiers deviennent alors vides dans le conteneur addc, ce qui fait échouer free, psutil et ensuite Salt avec KeyError: b'MemTotal:'.

Le retour à kernel.yama.ptrace_scope=1, suivi d'un redémarrage de l'hôte, restaure le fonctionnement normal de LXCFS et des tests clients Linux.

proposition =>
Deja géré par eole-common => /usr/share/eole/creole/distrib/sysctl.conf
Dans eole-common modifier la dernière ligne du fichier eole-common/tmpl/sysctl.conf pour remplacer 3 par 1

---
méthode
---

1. démarrage d'un amonecole etb3, connexion ssh addc, et lancement meminfo
2. logs amonecole : ptrace attach of "head -n 5 /proc/meminfo" was attempted by "/usr/bin/lxcfs /var/lib/lxcfs"
en cherchant on voit des limitation a YAMA => https://docs.kernel.org/admin-guide/LSM/Yama.html
or l'amonecole utilise justement : kernel.yama.ptrace_scope = 3, cas ou => citation "no processes may use ptrace with PTRACE_ATTACH nor via PTRACE_TRACEME. Once set, this sysctl value cannot be changed."

pour voir ce paramètre : sysctl -n kernel.yama.ptrace_scope

3. des incohérences dans le code ?

```
/etc/sysctl.conf:56:kernel.yama.ptrace_scope=3
/etc/sysctl.d/99-sysctl.conf:56:kernel.yama.ptrace_scope=3
/etc/sysctl.d/10-ptrace.conf:22:kernel.yama.ptrace_scope = 1
```

Le fichier chargé le plus tard l'emporte : la valeur 3 écrase donc la valeur Ubuntu 1.

```
lrwxrwxrwx 1 root root   14 juin   5 17:36 /etc/sysctl.d/99-sysctl.conf -> ../sysctl.conf
```

4. garder pour trace :

```
root@amonecole:~# /usr/lib/systemd/systemd-sysctl --cat-config |
grep -nE '(^# /|kernel\.yama\.ptrace_scope)'
1:# /usr/lib/sysctl.d/10-apparmor.conf
17:# /etc/sysctl.d/10-bufferbloat.conf
27:# /etc/sysctl.d/10-console-messages.conf
31:# /etc/sysctl.d/10-ipv6-privacy.conf
45:# /etc/sysctl.d/10-kernel-hardening.conf
57:# /proc/modules, etc), and this setting can censor the addresses. A value
72:# /etc/sysctl.d/10-magic-sysrq.conf
```

```
100:# /etc/sysctl.d/10-map-count.conf
105:# /etc/sysctl.d/10-network-security.conf
113:# /etc/sysctl.d/10-ptrace.conf
135:kernel.yama.ptrace_scope = 1
137:# /etc/sysctl.d/10-zeropage.conf
148:# /etc/sysctl.d/30-lxc-inotify.conf
159:# /usr/lib/sysctl.d/50-bubblewrap.conf
164:# /etc/sysctl.d/50-bubblewrap.conf and change the value of this parameter
168:# /usr/share/doc/bubblewrap/README.Debian
171:# /usr/lib/sysctl.d/50-pid-max.conf
189:# /etc/sysctl.d/99-eole-dirtyfrag.conf
192:# /usr/lib/sysctl.d/99-protect-links.conf
204:# /etc/sysctl.d/99-sysctl.conf
260:kernel.yama.ptrace_scope=3
```

5. test :

on change le 3 en 1 dans /usr/share/eole/creole/distrib/sysctl.conf, reconfigure et on validation :

```
grep -n 'kernel.yama.ptrace_scope' \
    /etc/sysctl.conf \
    /etc/sysctl.d/99-sysctl.conf \
    /etc/sysctl.d/10-ptrace.conf
```

Application des modif, il faut obligatoirement redémarrer le serveur pour un changement de valeur de kernel.yama.ptrace_scope :

reboot

contrôle des modif :

sysctl kernel.yama.ptrace_scope

résultat attendus : kernel.yama.ptrace_scope = 1

deux terminaux, un pour amonecole, un pour addc

sur amonecole :
journalctl -u lxcfs -f

ssh addc après l'affichage continue des logs :

```
wc -c /proc/meminfo /proc/cpuinfo /proc/stat
head -n 5 /proc/meminfo
free -m
```

résultat :

amonecole :
pas de retour dans les logs : dpkg -S /etc/sysctl.d/10-ptrace.conf

addc :

```
root@addc:~# wc -c /proc/meminfo /proc/cpuinfo /proc/stat
1531 /proc/meminfo
5896 /proc/cpuinfo
1276 /proc/stat
8703 total
```

```
root@addc:~# head -n 5 /proc/meminfo
MemTotal:        8127308 kB
MemFree:         7310976 kB
MemAvailable:    7512800 kB
Buffers:               0 kB
Cached:           201824 kB
root@addc:~# free -m
               total        utilisé      libre     partagé tamp/cache   disponible
Mem:            7936         600        7139           3         197        7336
Échange:           0           0           0
```

Demandes liées:

Lié à Distribution EOLE - Scénario #37495: "sysctl -p" VS "sysctl --system"	**Nouveau**

Révisions associées

Révision 4e519877 - 31/08/2026 15:25 - Benjamin Bohard

Revert "CVE ssh-keysign-pwn #37466"

Le noyau intègre les corrections nécessaires.

Ref #37560

This reverts commit de48445c1589af3528f459f4d9af42b4d747123a.

Révision dac0ab71 - 01/09/2026 16:35 - Joël Cuissinat

Revert "CVE ssh-keysign-pwn #37466" (jammy)

Le noyau intègre les corrections nécessaires.

Ref #37560

This reverts commit de48445c1589af3528f459f4d9af42b4d747123a.

Historique

#1 - 21/07/2026 11:25 - Ludwig Seys

- Statut changé de Nouveau à À valider

#2 - 21/07/2026 15:51 - Ludwig Seys

le problème étant que le précédent commit pour imposer cette valeurs à 3 réponds à une faille :

Il s'agit de la CVE-2026-46333, surnommée ssh-keysign-pwn. Une vulnérabilité du noyau Linux dans le mécanisme ptrace, permettant à un utilisateur local non privilégié de récupérer des informations sensibles depuis certains processus privilégiés en fin d'exécution. Le démonstrateur utilisait notamment /usr/lib/openssh/ssh-keysign pour exposer les clés privées SSH de l'hôte.
source : https://ubuntu.com/blog/ssh-keysign-pwn-linux-vulnerability-fixes-available?utm_source=chatgpt.com

Il faut donc au préalable vérifier que nous avons bien la version du noyau corrigeant cette faille avant de retirer le paliatif

#3 - 21/07/2026 15:57 - Ludwig Seys

- % réalisé changé de 80 à 90

la faille existe pour 6.8.0-124
l'amonecole testé est en 6.8.0-136.136

la logique correcte serait probablement :

- conserver 3 sur un noyau vulnérable ;
- revenir à 1 lorsque le noyau correctif est installé ;
- ou supprimer complètement la surcharge EOLE et laisser la valeur Ubuntu de /etc/sysctl.d/10-ptrace.conf, qui est déjà 1.

Autrement dit, si tous les noyaux supportés par EOLE 2.10 sont maintenant corrigés, le mieux pourrait être de supprimer ces deux lignes du template :

1. CVE ssh-keysign-pwn #37466
   kernel.yama.ptrace_scope=3

La configuration Ubuntu reprendrait alors naturellement la main avec sa conf par défaut :

kernel.yama.ptrace_scope = 1

#5 - 31/08/2026 14:24 - Joël Cuissinat

- Lié à Scénario #37495: "sysctl -p" VS "sysctl --system" ajouté

#6 - 31/08/2026 15:34 - Benjamin Bohard

Une correction est proposée en mise à jour des noyaux pour les versions concernées : https://ubuntu.com/security/CVE-2026-46333

On peut retirer le patch de sécurité de sysctl.conf.

#7 - 10/09/2026 10:33 - Laurent Gourvenec

- Statut changé de À valider à Résolu

- % réalisé changé de 90 à 100

#8 - 10/09/2026 15:46 - Klaas TJEBBES

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0