SECURELEVEL(7) Manuel de Référence d'OpenBSD SECURELEVEL(7)

NOM

securelevel - niveau de sécurité du noyau et ses effets.

DESCRIPTION

Le noyau d'OpenBSD fournit quatre niveaux de sécurité système :

- -1 *Mode non sécurisé permanent*
  - init(8) n'essaiera pas d'élever le niveau de sécurité
  - ne peut être mis en place qu'avec sysctl(8) quand le système est en mode non sécurisé
  - à par cela, les effets sont identiques à ceux du niveau de sécurité 0
- 0 *Mode non sécurisé*
  - utilisé durant la séquence d'amorçage et quand le système est en mode mono-utilisateur
  - il est possible de lire et d'écrire sur tous les périphériques selon leurs autorisations d'accès
  - les drapeaux de fichier de niveau système peuvent être effacés
- 1 *Mode sécurisé*
  - mode par défaut quand le système est en mode multi-utilisateurs
  - impossible d'abaisser le niveau de sécurité, sauf par init
  - impossible d'écrire dans */dev/mem* et */dev/kmem*
  - les périphériques d'accès aux données brutes des disques avec des systèmes de fichiers montés sont en lecture seule
  - impossible de retirer les drapeaux de fichiers immuable et ajout seul
  - impossible de charger ou de décharger des modules noyau
  - impossible de modifier la variable sysctl(8) *fs.posix.setuid*
  - impossible de modifier la variable sysctl(8) *net.inet.ip.sourceroute*
  - impossible de modifier la variable sysctl(8) *machdep.kbdreset*
  - impossible d'élever les variables sysctl(8) *ddb.console* et *ddb.panic*
  - impossible d'élever la variable sysctl(8) *machdep.allowaperture*
- 2 *Mode fortement sécurisé*
  - tous les effets du niveau de sécurité 1
  - les périphériques d'accès aux données brutes des disques sont en lecture seule, qu'ils soient montés ou non
  - settimeofday(2) et clock_settime(2) ne peuvent pas fixer une date passée ou trop proche d'un dépassement
  - impossible de modifier les règles de filtrage et de NAT de pf(4)

Le niveau de sécurité fournit des moyens commodes pour “verrouiller” au à un degré convenable pour son environnement. Il est normalement fixé au démarrage par le biais du script rc.securelevel(8) ; par ailleurs l'administrateur peut augmenter le niveau de sécurité à tout moment en modifiant la variable sysctl(8) *kern.securelevel*. Cependant, seul init(8) peut le baisser une fois que le système est entré en mode sécurisé. Un noyau construit avec l'**option INSECURE** dans le fichier config fonctionnera par défaut en mode non sécurisé permanent.

Le mode fortement sécurisé peut sembler draconien, mais il a pour but d'être la dernière ligne de défense quand le compte administrateur est compromis. Ses effets écartent le contournement des

drapeaux de fichier par la modification directe des périphériques d'accès aux données brutes des disques, ou par l'effacement d'un système de fichiers au moyen de newfs(8). En plus, il peut limiter les dégâts potentiels d'un “pare-feu” compromis en interdisant la modification de règles de filtrage de paquets. Le fait d'interdire l'horloge du système d'être réglée à une date antérieure est un secours pour l'analyse post-mortem, et cela aide à garantir l'intégrité des journaux. Le chronométrage de précision n'est pas affecté parce que l'horloge peut toujours être ralentie.

Puisque le niveau de sécurité est modifiable avec le debugger ddb(4) intégré au noyau, un moyen commode de le verrouiller (si présent) est fourni dans les niveaux de sécurité 1 et 2. On peut le faire en fixant *ddb.console* et *ddb.panic* à 0 avec l'utilitaire sysctl(8).

FICHIERS

- /etc/rc.securelevel commandes à exécuter avant que le niveau de sécurité ne change

VOIR AUSSI

chflags(2), settimeofday(2), mem(4), options(4), init(8), rc(8), sysctl(8)

HISTORIQUE

La page du manuel **securelevel** est apparue la première fois dans OpenBSD 2.6.

ANOMALIES

Il se peut que la liste des effets d'un niveau de sécurité soit incomplète.

OpenBSD 4.4 1 juin 2007 2