

Microsoft pousse IPE, module de sécurité Linux

Microsoft a livré les détails d'un projet maison de LSM (Linux Security Module) dans un [document](#) technique repéré par [ZDNet](#).

Le [noyau Linux](#) supporte différents LSM, dont SELinux (Security-Enhanced Linux) et AppArmor parmi les plus connus. Microsoft, contributeur et utilisateur de Linux comme socle technique de différentes initiatives, a nommé son projet IPE (Integrity Policy Enforcement).

Celui-ci est conçu pour renforcer l'intégrité du code pour le noyau Linux, afin de garantir que « tout code en cours d'exécution (ou fichiers en cours de lecture), est identique à la version qui a été créée par une source de confiance », a souligné Microsoft sur [GitHub](#).

IPE Core

Certains LSM existants manquent d'une mesure de vérification au moment de l'exécution des binaires, selon la firme Redmond. IPE vise donc à combler cette lacune. Si des binaires ont été modifiés par un attaquant, IPE est conçu pour en bloquer l'exécution.

IPE inclut deux composants principaux : IPE Core (configurable) et IPE Properties (des attributs fournis par le noyau pour évaluer les fichiers).

« Idéalement, un système qui exploite IPE n'est pas destiné à un usage informatique général et n'utilise pas de configuration ou de logiciel construit par un tiers », a précisé l'éditeur.

En outre, le LSM promu par Microsoft est conçu pour des cas spécifiques, comme des systèmes embarqués, dans lesquels la sécurité est prioritaire, et les administrateurs systèmes ont le contrôle total.