CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-08(14)

Droit d’accès minimal

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-08(14) — Droit d’accès minimal (PbMM)

Énoncés :

Mettre en place le principe de conception sécurisée du droit d’accès minimal dans les [Affectation : systèmes ou composants de systèmes désignés par l’organisation].

Responsable : Aucun

Discussion :

Le principe de droit d’accès minimal repose sur le fait que l’on doit affecter suffisamment de privilèges à chaque composant du système pour accomplir ses fonctions, mais sans plus. L’application du principe de droit d’accès minimal limite la portée des actions du composant, ce qui a deux conséquences désirées : l’incidence sur la sécurité d’un composant sera moindre advenant une défaillance, une corruption ou une mauvaise utilisation et il sera plus facile de procéder à l’analyse de la sécurité du composant. Le principe de droit d’accès minimal est un principe omniprésent qui se reflète dans tous les aspects de la conception d’un système sécurisé. Les interfaces utilisées pour appeler les capacités du composant ne sont accessibles que par certains sous-ensembles de la population d’utilisatrices et utilisateurs, et la conception du composant prend en charge un degré de granularité suffisamment précis pour assurer la décomposition des privilèges. Par exemple, dans le cas d’un mécanisme de vérification, on pourrait retrouver une interface pour la ou le gestionnaire des vérifications, qui configure les paramètres de vérification, une interface pour l’exploitante ou exploitant des vérifications, qui s’assure que les données de vérification sont collectées et stockées en toute sécurité et, pour finir, une autre interface pour la réviseuse ou le réviseur des vérifications, qui doit afficher les données de vérification collectées sans toutefois effectuer d’opérations à partir de ces données. En plus de ses manifestations dans l’interface du système, le principe de droit d’accès minimal peut être utilisé comme principe directeur pour la structure interne du système en tant que tel. Un aspect du droit d’accès minimal interne est de construire des modules de manière à ce que seules les fonctions d’un module puissent effectuer des opérations directes sur les éléments encapsulés par ce module. Il est possible d’accéder indirectement aux éléments externes à un module susceptibles d’être touchés par l’exploitation de ce module dans le cadre d’une interaction (par exemple, lors d’un appel de fonction) avec le module qui contient ces éléments. Un autre aspect du droit d’accès minimal interne veut que la portée d’un module ou d’un composant donné comprenne uniquement les éléments du système qui sont nécessaires pour son fonctionnement et que les modes d’accès des éléments (par exemple, lecture, écriture) soient minimaux. La minimisation des fonctions qui utilisent des privilèges élevés (par exemple, la restriction des outils et des fonctions qui s’exécutent en mode noyau) est un exemple de droit d’accès minimal dans le développement logiciel.