UAC Virtualization

Notions de base

Sous Windows 10 (ce qui, en principe, était déjà valable depuis Windows VISTA), il n'est pas possible d'accéder à certains emplacements des programmes avec des droits d'utilisateur normaux. Cette restriction, consistant à ne pouvoir modifier ces fichiers et chemins d'accès qu'avec les droits d'administrateur, fait partie du concept de sécurité de Windows et est désignée sous les termes User Account Control (UAC, contrôle du compte de l'utilisateur).

Cela concerne notamment :

- C:\Windows
- C:\Program Files
- C:\Program Files (x86)

et éventuellement d'autres chemins associés au système.

En outre, certains types de fichiers ne peuvent en aucun cas être modifiés sans droits d'administrateur ; c'est le cas, entre autres, de ceux qui suivent :

- EXE
- VBA
- BAT

Il s'agit, pour la plupart d'entre eux, de fichiers exécutables qui peuvent comporter, dans le pire des cas, des codes malveillants. Pour plus d'informations, reportez-vous au document de Mark Russinovich.

Le problème

Cette situation pose le problème suivant : la pratique établie visant à enregistrer les données utilisateur ainsi que, par exemple, les paramètres de base et les options à l'emplacement des programmes n'est plus envisageable tant que le programme est exécuté sans droits d'administrateur. Il en va de même pour la solution la plus couramment utilisée pour enregistrer les paramètres dans le registre. Il ne suffit même pas d'être connecté en tant qu'administrateur ; le programme doit être expressément lancé avec des droits élevés, à l'aide du menu bouton droit et en sélectionnant « Exécuter en tant qu'administrateur ».

En ce qui concerne le programme Metric, cela signifie que, désormais, les paramètres de base tels que les systèmes de mesure, le calibrage, la durée d'exposition ainsi que la connexion des tables de mesure et tables motorisées, qui ont tous été enregistrés dans le fichier « Metric.opt » du chemin d'accès aux programmes, ne peuvent plus être modifiés par quiconque. Il y a toutefois une exception : le lancement du programme avec des droits élevés. Néanmoins, le niveau de sécurité s'en trouverait diminué s'il est possible qu'un utilisateur normal lance le programme Metric avec des droits d'administrateur.

Pour remédier à ces problèmes, Microsoft a inventé la technologie « Virtualisation UAC ». Si un programme ne dispose pas de droits d'écriture ou de modification d'un fichier dans le répertoire souhaité, une copie est alors créée à un endroit particulier et cette copie, en lieu et place de l'original (même si le fichier ne se trouve plus dans le répertoire cible), apparaît virtuellement dans le répertoire cible.

Exemple : vous êtes connecté en tant que « YouAsAUser » avec des droits d'utilisateur normaux et vous souhaitez enregistrer les paramètres sur Metric.opt. Étant donné que vous n'êtes pas autorisé à enregistrer sous « C:\Program Files (x86)\Metric\Metric.opt », Windows sauvegarde une copie de ce fichier sous : C:\Users*YouAsAUser*\AppData\Local\VirtualStore\Program Files (x86)\Metric\Metric.opt.

C:\Users*YouAsAUser*\AppData\Local\VirtualStore\Program Files (x86)\Metric\Metric.opt

La virtualisation UAC sauvegarde le fichier à un tout autre endroit.

Peu importe que l'administrateur ait modifié vos droits d'écriture sous « C:\Program Files (x 86) \Metric », Windows détecte un chemin d'accès critique et effectue automatiquement la virtualisation pour vous. Comme il a été susmentionné, il y a une exception : si vous démarrez expressément le programme Metric avec des droits élevés, ce qui est interdit pour des raisons de sécurité.

Si vous souhaitez maintenant poursuivre et charger le fichier depuis « C:\Program Files (x86)\Metric\Metric.opt », Windows charge en fait le fichier depuis le VirtualStore.

En votre qualité d'utilisateur, cela se révèle très pratique. Vous disposez ainsi d'une sécurité élevée grâce à la virtualisation UAC et vous pouvez également enregistrer les données comme d'habitude, là où votre programme est installé.

Si, pendant ce temps, un autre utilisateur se connecte en tant que « YourCollegue », deux choses se produisent :

1. Votre collègue peut, lors du premier démarrage du programme, lire le fichier d'origine de Metric.opt.
2. Lors de l'enregistrement, votre collègue génère dans son propre VirtualStore une nouvelle copie de Metric.opt, que lui seul peut voir.

Vous avez donc désormais trois fichiers Metric.opt différents : celui installé à l'aide du CD, votre copie personnelle et la copie de votre collègue. Néanmoins, vous ne verrez qu'un seul fichier Metric.opt à l'emplacement de l'application. Les seules différences seront probablement la taille du fichier et sa date de création.

Avantage de votre point de vue : vous êtes sûr que votre collègue ne peut pas modifier vos paramètres. Inconvénient : si certains paramètres de base, tels que le calibrage, doivent être modifiés, cette opération devra être effectuée par tous les employés séparément, ce qui peut représenter beaucoup de travail si de nombreux employés travaillent sur cette machine.

Si, dans votre cas, cette virtualisation UAC s'avérait être un problème, il est possible d'y remédier comme suit.

La solution UAC File Exclude

Comme mentionné plus haut, il existe certains types de fichiers pour lesquels la virtualisation UAC n'est pas appliquée. Si l'on ajoute maintenant le type de fichier « OPT » à cette liste, on empêche alors la virtualisation de Metric.opt (et de tous les autres fichiers dotés de l'extension opt)..

L'utilisateur individuel ne peut plus modifier aucun paramètre. Seul un administrateur qui a expressément lancé le programme Metric avec des droits élevés peut modifier les paramètres. S'il s'agit bien de la solution recherchée, ça y est, c'est fini. Le fichier « uac opt exclusion.reg » joint comprend l'entrée de registre suivante, qui effectue le travail pour vous et ajoute l'extension de fichier OPT aux extensions exclues.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\luafv\Parameters]
"ExcludedExtensionsAdd"=hex(7):6f,00,70,00,74,00,00,00,00,00
```

Ces caractères hexadécimaux codifient la chaîne « OPT » au format DBCS et une chaîne vide. En double-cliquant sur le fichier et en validant toutes les requêtes de l'UAC, l'entrée dans le registre est effectuée. Ensuite, le système doit être redémarré pour que les modifications soient appliquées.

La solution avancée « Droits d'écriture »

Si les utilisateurs normaux souhaitent également modifier les paramètres du programme Metric, ils doivent de surcroît disposer des droits d'écriture sur le chemin d'installation de Metric (« C:\Program Files (x 86) \Metric »). Dans ce cas, « Modifier/Changer » devrait être suffisant étant donné qu'il n'est pas nécessaire d'enregistrer tout un nouvel ensemble de paramètres dans un autre fichier. L'administrateur peut ainsi configurer les droits minimaux et n'est pas obligé d'accorder expressément un « accès complet » à cet emplacement.