Wirtualizacja UAC

Podstawowe koncepcje

Niektóre ścieżki programu w systemie Windows (zasadniczo już występujące od wersji Windows VISTA) mogą nie zapisywać się prawidłowo ze standardowymi prawami użytkownika. Ograniczenie to, stanowiące, że te pliki i ścieżki i mogą być zmieniane wyłącznie przez osoby z prawami administratora, stanowi element koncepcji zabezpieczeń w systemie Windows, o nazwie kontrola konta użytkownika (User Account Control, UAC).

Dotyczy to w szczególności następujących ścieżek

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

i być może innych ścieżek o krytycznym znaczeniu dla systemu.

Ponadto niektóre typy plików mogą być zmieniane wyłącznie przez użytkowników z prawami administratora, między innymi

- EXE
- VBA
- BAT

stanowiące głównie pliki wykonywalne, które mogą w najgorszym razie zawierać złośliwy kod. Więcej szczegółowych informacji na ten temat można znaleźć w dokumencie Marka Russinovicha.

Problem

Przy zastosowaniu tej koncepcji nie jest możliwe wykorzystanie ustalonej praktyki w celu zapisywania takich danych użytkowników, jak podstawowe ustawienia i opcji ścieżki programu, gdy program nie został uruchomiony z prawami administratora. Powszechnie stosowana metoda zastępcza zapisywania ustawień w rejestrze cierpi z tego samego powodu. Nie wystarczy nawet być zalogowanym jako administrator; program musi zostać uruchomiony z rozszerzonymi prawami, z użyciem prawego kliknięcia myszy i polecenia „uruchom jako administrator”.

W przypadku programu Metric teraz nie jest możliwe zapisanie podstawowych ustawień, jak systemy pomiarowe, kalibracja, czas ekspozycji lub połączenie stołów pomiarowych czy napędów silników – wszystkie zapisywane w Metric.opt w ścieżce programu – z jednym wyjątkiem: konieczne jest uruchomienie z rozszerzonymi prawami. To spowoduje jednak z kolei likwidację zabezpieczeń, jeśli zwykły użytkownik będzie mógł uruchomić program z prawami administratora.

Aby zlikwidować te problemy, firma Microsoft stworzyła technikę o nazwie „wirtualizacja UAC”. Jeśli program nie dysponuje prawami do zapisu lub zmiany pliku w żądanej ścieżce, kopia tego pliku jest zapisywana w specjalnej lokalizacji i ta kopia (nawet nie plik istniejący w katalogu docelowym) jest wirtualnie wyświetlana w katalogu docelowym.

Przykład: Jesteś zalogowany jako „TyJakoUżytkownik” z normalnymi prawami użytkownika i chcesz zapisać ustawienia w Metric.opt. Ponieważ nie wolno Ci tego zrobić w „C:\Program files (x86)\Metric\Metric.opt“, system Windows zapisuje kopię tego pliku w

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

Wirtualizacja UAC zapisuje plik w zupełnie nowym miejscu.

Nie ma znaczenia, czy administrator zmienił Twoje prawa zapisu do „C:\Program files (x86)\ Metric. System Windows automatycznie rozpoznaje ścieżkę krytyczną i wykonuje dla Ciebie wirtualizację. Jak wspomniano powyżej, jedyny wyjątek to taki, kiedy jednoznacznie uruchamiasz program Metric z rozszerzonymi prawami, co jest zabronione z przyczyn związanych z bezpieczeństwem.

Jeśli chcesz kontynuować i pobrać plik z „C:\Program files (x86)\Metric\Metric.opt“, system Windows pobierze ten plik z magazynu wirtualnego.

Dla indywidualnego użytkownika jest to wyjątkowo wygodne. Z jednej strony dysponujesz wysokim poziomem zabezpieczeń dzięki wirtualizacji UAC, a z drugiej strony możesz postępować zgodnie z przyzwyczajeniem i zapisywać swoje pliki i ustawienia tam, gdzie zainstalowano program.

Jeśli w tej sytuacji inny użytkownik zaloguje się jako „TwójKolega”, dojdzie do dwóch rzeczy:

1. Twój kolega przeczyta przy pierwszym uruchomieniu programu Metric oryginalnie zainstalowany plik Metric.opt,
2. W chwili zapisu Twój kolega stworzy nowy plik Metric.opt w swoim własnym magazynie wirtualnym i tylko on będzie widzieć jego kopię.

Teraz mamy trzy różne pliki Metric.opt: Jeden zainstalowany z płyty CD, Twoją prywatną kopię i kopię prywatną Twojego kolegi, a wszystkie można zobaczyć w jednym pliku Metric.opt w ścieżce aplikacji. Prawdopodobnie będą się różnić jedynie rozmiarem i godziną utworzenia.

Istotna zaleta polega na tym, że kolega nie może zmieniać Twoich ustawień. Jeśli jednak konieczna jest zmiana pewnych ustawień podstawowych, jak kalibracja, należy to zrobić dla każdego z pracowników osobna, co może być dość pracochłonne, jeśli wielu pracowników korzysta z maszyny.

Jeśli w Twoim przypadku wirtualizacja jest problemem, można go rozwiązać w poniżej opisany sposób.

Rozwiązanie z plikiem wyłączeń UAC

Jak wspomniano powyżej, istnieją typy plików, które nie są poddawane wirtualizacji przez UAC. Jeśli dodasz OPT do listy typów plików, wirtualizacja dla pliku Metric.opt (i wszystkich innych plików z rozszerzeniem *.opt) nie będzie się już odbywać.

Zwykły użytkownik nie może już zmieniać ustawień. Tylko administrator, który jednoznacznie uruchamia program Metric z rozszerzonymi prawami, może je zmieniać. Jeśli to jest dla Ciebie właściwe rozwiązanie, nie musisz już dalej szukać. Plik „uac opt exclusion.reg” zawiera wpis rejestru, który wykona zadanie za Ciebie, dodając rozszerzenie *.opt do wyłączonych rozszerzeń.

```
Edytor rejestru systemu wersja 5.00

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

To znaki kodu szesnastkowego dla ciągu znaków „OPT” w formacie DBCS i pusty ciąg. Klikając dwa razy plik i akceptując wszystkie pytania UAC spowodujesz dokonanie tego zapisu w rejestrze, a ponowne uruchomienie systemu spowoduje wprowadzenie zmian.

Rozwiązanie rozszerzone z „pozwoleniem zapisu”

Jeśli zwykli użytkownicy mają zmieniać ustawienia programu Metric, muszą otrzymać prawo zapisu w ścieżce instalacyjnej programu Metric („C:\Program files (x86)\Metric”). W tym przypadku „modyfikacja/zmiana” wystarczy, gdyż zapisywanie całkowicie nowego zestawu ustawień w innym pliku nie jest konieczne. Administrator może więc przyznać minimalne prawa i nie musi przyznawać pełnego dostępu do ścieżki.