

20 February 2007

By: Marius Oiaga, Technology News Editor

## **Symantec: Don't Trust Windows Vista UAC Prompts!**

### *Because of the RunLegacyCPL Elevated.exe*



Symantec has analyzed the User Account Control in Windows Vista and has presented the verdict. Do not trust UAC prompts. In this regard, Symantec has also provided an example of how the User Account Control can be abused in order to fool the user in elevating a malicious process. At the basis of this is the fact that the UAC does not provide a security boundary or direct protection, but only a chance for the user to verify an action before allowing it to take place. "The issue I discovered was that the binary RunLegacyCPL Elevated.exe, [which] is designed to provide backward compatibility by allowing legacy Windows Control Panel plug-ins to run with full administrative privileges. What's the drama? I hear you say. The problem stems from the fact that RunLegacyCPL Elevated.exe takes as one of its parameters an arbitrary DLL with a particular export. The DLL has to export the CPIApplet function, which is then called with a number of different parameters depending on the action being performed," explained Ollie Whitehouse, Symantec Security Response Researcher. If you want to find out more about how you can add run levels to legacy control panel applets in Windows Vista via shimming, then click [here](#). But the bottom line is that shimming can also backfire. A malicious piece of code can drop a malformed CPL file onto a disk location where it can write and then call RunLegacyCPL Elevated.exe. With the malicious CPL as a parameter, the Vista user will be presented with a UAC prompt that comes from Windows, and not from a third party application. Authorizing such an elevation would give administrative privileges to the malware. "So while Microsoft may use the word trust when in relation to UAC in some of their documentation with statements such as - "The following illustration details the elevation prompt logic for corresponding levels of trust." - in actual fact, even the data these UAC prompts provide you with can't be trusted," Whitehouse added.