The WMI root node is just a node in the WMI namespace

devblogs.microsoft.com/oldnewthing/20180327-00

March 27, 2018

Raymond Chen

A security vulnerability report arrived that went roughly like this:

> There is a serious zero-day security vulnerability in the `WMIC.EXE` program. It does not check whether the user has administrative privileges before granting access. Simply sign in as a standard user and run the `wmic` program. Observe from the prompt that it gives you root access.
>
> ```
> C:\> del config.sys
> Access is denied
>
> C:\> wmic
> wmic:root\cli> cdrom get description, drive
> Description   Drive
> CD-ROM Drive  D:
> ```

The WMIC prompt looks like this:

```
wmic:root\cli>
```

This is telling you that your current location (which WMI calls a *role* for some reason) is the `cli` node in the root of the WMI namespace. You can change this by typing

```
wmic:root\cli> /ROLE:..\cimv2
wmic:root\cimv2>
```

We suspect that the finder saw the word *root* and assumed it had the same meaning here as it does in Unix. In Windows, the administrator account is called *Administrator*, not *root*.

Their screen shot shows that they don't have administrator privileges when they started (because they can't delete the file `C:\config.sys`). From inside the `WMIC` tool, they printed information about the CD-ROM drives, but that operation doesn't require administrator privileges, so that isn't proof that any elevation occurred.

Running the `WMIC` program doesn't change your security level. If you don't have administrator privileges, then you still cannot do things like, say, delete system files.

```
wmic:root\cli>datafile where name="C:\\config.sys" delete
Delete '\\PC\ROOT\CIMV2:CIM_DataFile.Name="c:\\config.sys"' (Y/N/?)? y
Deleting instance \\PC\ROOT\CIMV2:CIM_DataFile.Name="c:\\config.sys"
ERROR:
Description = Access denied
```

Raymond Chen

Follow