

## Re: Auto-update of an application, permission problem in "Program Files"

---

*Source:*

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2007-06/msg00116.ht>

---

- *From:* [jetan@xxxxxxxxxxxxxxxxxxxxxx](mailto:jetan@xxxxxxxxxxxxxxxxxxxxxx) ("Jeffrey Tan[MSFT]")
  - *Date:* Tue, 12 Jun 2007 04:20:16 GMT
- 

Hi Francois,

Thanks for your feedback.

Yes, using a dedicated service or process will gain better security.

If you do not use a separate process, your normal application which runs under your interactive user account have to gain write permission to the "Program Files" directory. However, in Vista, the normal interactive token is a filtered normal user account token by default. So you have to assign normal user write permission to the "Program Files" directory. This definitely gives all other normal user account processes write permission to the "Program Files" directory. It means any hacker code runs under a user account can modify or replace your code in "Program Files" directory, which is really a security hole.

With a high priviledge process for this write operation, there is no need to lower the DACL security setting of your "Program Files" directory by giving write permission to normal user tokens/accounts. Only your known-good high priviledge process have write permission to the "Program Files" directory. The attack surface is guaranteed to be small. So it is more secure.

If you do no want to afford the complexity of coding a Windows Service, I would suggest you to take the solution of the last paragraph in my first reply, I paste it below:

"A variation of this solution is coding a separate high-priviledge updating application. While asking for updating, your normal application can use ShellExecute API with "runas" parameter to run the updating application under the full administrator token, which has the permission of writting to the "Program Files". This approach has the advantage of prompting the end user with a consent dialog for updating, which aligns with Vista UAC behavior. See the "Run as administrator" section in the link below for details:

[http://weblogs.asp.net/kennykerr/archive/2006/09/29/Windows-Vista-for-Developers-\\_1320\\_-Part-4-\\_1320\\_-User-Account-Control.aspx](http://weblogs.asp.net/kennykerr/archive/2006/09/29/Windows-Vista-for-Developers-_1320_-Part-4-_1320_-User-Account-Control.aspx)"

Re: Auto-update of an application, permission problem in "Program Files"

If you still have anything unclear or unsure, please feel free to tell me, thanks.

Best regards,  
Jeffrey Tan  
Microsoft Online Community Support

=====  
Get notification to my posts through email? Please refer to  
<http://msdn.microsoft.com/subscriptions/managednewsgroups/default.aspx#notifications>.

Note: The MSDN Managed Newsgroup support offering is for non-urgent issues where an initial response from the community or a Microsoft Support Engineer within 1 business day is acceptable. Please note that each follow up response may take approximately 2 business days as the support professional working with you may need further investigation to reach the most efficient resolution. The offering is not appropriate for situations that require urgent, real-time or phone-based interactions or complex project analysis and dump analysis issues. Issues of this nature are best handled working with a dedicated Microsoft Support Engineer by contacting Microsoft Customer Support Services (CSS) at  
<http://msdn.microsoft.com/subscriptions/support/default.aspx>.

=====  
This posting is provided "AS IS" with no warranties, and confers no rights.