

Re: Administrator elevation via RPC fails on Vista, why?

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2006-03/msg00186.htm>

- *From:* Stefan Kuhr <kustt110@xxxxxx>
 - *Date:* Thu, 09 Mar 2006 12:33:10 +0100
-

Hi Skywing,

Skywing wrote:

IIRC, any privileges that are in the token but not enabled get stripped away across impersonation boundaries, so – you might try turning on all privileges present before the security context is captured by impersonating, transmitting the "real" privilege state with an RPC message or whatnot, then restoring the original privilege state on the impersonating end when you get the appropriate message.

(Note that I don't really know if this will do what you need to do in Vista – however I have successfully used techniques similar to this to get the "important" parts of the token saved across an impersonation boundary in <=Windows Server 2003. So it's probably worth a shot, at least.)

I am aware of the fact that those privileges that the client process has not explicitly enabled before making the RPC are stripped from the token that the impersonator gets. Actually, my test client tries to enable all possible privileges. However, privileges are not the primary problem with admin elevation on Vista. The restricted token of a non-elevated administrator manifests itself first and foremost in the group sid of builtin\administrators being SE_GROUP_USE_FOR_DENY_ONLY (it is SE_GROUP_OWNER in a full token) and two new SIDs of type label (which apparently is not yet documented). These two label SIDs can successfully be elevated to the values in a full admin token using SetTokenInformation(..., TokenIntegrityLevel...) and (obviously) well-known SID using the approach outlined here:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/IETechCol/dnwebgen/ProtectedMode.asp>

but the group SID for builtin\administrators with SE_GROUP_USE_FOR_DENY_ONLY cannot be replaced because SetTokenInformation(..., TokenGroups,) won't succeed (if that would

Re: Administrator elevation via RPC fails on Vista, why?

work, any service running as LocalSystem could masquerade as any user).

Anyway, thanks for helping.

—
Stefan

.