

Re: [Full-disclosure] Microsoft Windows Vista/2003/XP/2000 file management security issues

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-03/msg00118.html>

- *From:* KJKHyperion <hackbunny@xxxxxxxxxxx>
 - *Date:* Fri, 09 Mar 2007 03:15:50 +0100
-

3APA3A wrote:

2. Conclusion:

[...]

hahaha. Seriously, the Windows security model is great and everything, but it has never been used consistently, _never_. It's an uphill battle. Take privileges for example: 64-bit namespace and barely above a dozen have been defined; two were overloaded and one recycled; and still no way to create arbitrary privileges. So to implement capability checks you perform group membership checks or make creative use of ACLs. Or take default device security. Or how sandboxing inexplicably breaks SSPI, making it close to useless. Or the countless hard-coded ACLs that make the complexity of the whole thing so unjustified you wonder why don't they just go with an "is administrator" bit. Or the total coolness that is Safer, truly a few hooks short of a filesystem firewall, and how criminally underused it is.

Then there's the compatibility issues.

PGP Desktop breaks sandboxing rather spectacularly (silent crashes in all sandboxed applications) because when its hook cannot open the shared memory object (created with whatever default ACL was specified for the PGPTray.exe process) it just tries to access the NULL pointer returned.

Sandboxing breaks the language bar – shared memory woes again. It has the common decency of not crashing or worse, it just sorta limps along a little. And the funny thing is, there _is_ a standard, documented way to perform access checks compatible with GUI security boundaries (it's not explicitly documented as such, but hey, we all come with a brain): all processes in interactive sessions receive a special group ("logon id") whose membership grants access to the display. It should be a _given_ for GUI hooks to use this mechanism, more so for GUI hooks developed by Microsoft – but the language bar developers amply proved to be a bunch of fucking cowboys anyway, and to Microsoft's credit they got it totally

Re: [Full-disclosure] Microsoft Windows Vista/2003/XP/2000 file management security issues

wrong in the Windows 2000 version of runas, but fixed it for Windows XP

A long time ago I tried to advocate making all files in one's own user profile non-executable by default, as a basic protection measure, and like all the ideas I try to push, I dogfooded it extensively. It subtly breaks a lot of innocent programs.

Other than completely isolating users, you cannot get any realistic form of security. Isolating users from each other and from administrators is the only scenario that has consistently been implemented and recognized. The rest is a wasteland of abandoned technology and wishful thinking

The problem you describe? it has a 1-bit fix, SE_DACL_PROTECTED. All files would be created by default with full access to owner and SYSTEM. You can have fat lots of fun trying to figure out what will break and how. A real solution would involve new DACL/SACL entries for directories that enforce "acceptable" security descriptors on the files contained therein. The same could work in the default DACL/SACL for tokens, enforcing policies for *all* objects created by that subject (yes, I put way too much thought in this. I am just gay for the Windows security model. You can't not love a model where a subject might not belong to the "world" group)

(ReadDirectoryChangesW on the other hand *is* a vulnerability, as it gives traverse *and* list acces but only requests traverse)

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>