

RE: [Full-Disclosure] M\$ – so what should they do?

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-06/0768.html>

From: Eric Paynter (eric_at_arcticbears.com)

Date: 06/22/04

To: full-disclosure@lists.netsys.com

Date: Mon, 21 Jun 2004 21:21:26 -0700 (PDT)

On Mon, June 21, 2004 3:55 pm, joe said:

- > *I have written several registry editor type apps for customers, it is*
- > *simply another API. For me writing a text editor is the same as writing a*
- > *registry editor, in fact, the classes I put together treat them both very*
- > *similarly from code use perspective.*

You missed one significant point, though. In my 15 years of computer programming, I have never **had** to write a text editor. Whereas, you have had to write **several** (your word) registry editors. And the only person who needs to know anything about a filesystem API is a compiler programmer. The rest of us mere humans use the standard library of `open()`, `close()`, `read()`, and `write()` commands if we want to access files programmatically.

One more thing, because of the complexity of the registry and removing it from the filesystem, in Windows, you need to learn the filesystem API (whatever that means to you) to get at the filesystem, the registry API to get at the registry, the COM API if you want to communicate between processes, and several application-specific APIs to programmatically configure most applications. In Unix systems, it's all treated as files. You use a common interface to use them all – `open()`, `close()`, `read()`, `write()`. How much simpler can it be? And the simpler it is, the less margin for error. And the less margin for error, the less risk of exploit. And that means better security... something to think about.

And before you say you **can** configure apps by directly editing the registry, removing the need to learn all of those unique APIs (although still leaving you without a nice local IPC interface), you'd better check your support agreement on that. Even Windows is not supported by MS if you directly edit the registry. Most app vendors say you're on your own too if you do that... So good luck! Any bad move in the registry is like open heart surgery. The box may never boot again – I know, I've done it more than once.

- > *10 people on one machine all load the same app... Here is where the pain*

Full-Disclosure: RE: [Full-Disclosure] M\$ – so what should they do?

- > *comes in. That could be a terrible waste of space and resources, but from*
- > *a security standpoint, maybe they should all maintain all of their own*
- > *info for each instance.... But*