It rather involved being on the other side of this airtight hatchway: If you grant users full control over critical files, then it's not the fault of the system for letting users modify them

devblogs.microsoft.com/oldnewthing/20100902-00

September 2, 2010

Raymond Chen

Today's dubious security vulnerability is another example of *If you reconfigure your computer to be insecure, don't be surprised that there's a security vulnerability*. This example comes from by an actual security vulnerability report submitted to Microsoft:

> I have found a critical security vulnerability that allows arbitrary elevation to administrator from unprivileged accounts.
>
> 1. Grant Full Control of the Windows directory (and all its contents and subdirectories) to Everyone.
> 2. Log on as an unprivileged user and perform these actions…

I can just stop there because your brain has already stopped processing input because of all the alarm bells ringing after you read that first step. That first step gives away the farm. If you grant control to the entire contents of the Windows directory to non-administrators, then don't be surprised that they can run around and do bad things! "If I remove all the locks from my doors, then bad guys can steal my stuff."

Yeah, so don't do that. This is not a security vulnerability in the door.

Bonus chatter

: There are many variations on this dubious security vulnerability. Actual vulnerability reports submitted to Microsoft include

- "First, grant world-write permission to this registry key…"
- "First, reconfigure Internet Explorer to allow scripting of ActiveX controls not marked safe for scripting…"
- "On a compromised machine, you can…"

That last one is impressive for its directness. “Starting on the other side of this airtight hatchway…”

Raymond Chen

Follow