Creating an object on the other side of the airtight hatchway isn't yet a security vulnerability

devblogs.microsoft.com/oldnewthing/20170130-00

January 30, 2017

Raymond Chen

A security vulnerability report came in that went something like this:

> UAC can be trivially circumvented as follows.
>
> 1. Sign in as a user who is a member of the Administrators group.
> 2. Run Task Manager.
> 3. Go to the Processes tab.
> 4. Click "Show processes from all users."
> 5. Task Manager will relaunch itself elevated without triggering a UAC prompt.
> 6. From the File menu, select Run.
> 7. Check the box "Create this task with administrator privileges."
> 8. Type any program name you wish and click OK.
> 9. Observe that the program is launched with elevated privileges and no UAC prompt was ever shown to the user.
>
> The security implications of this are wide-ranging.

Okay, let's see what happened here. You ran Task Manager, then elevated it (by clicking "Show processes from all users"), and then used that elevated Task Manager to launch more elevated processes. So far, nothing is actually wrong. You did manage to launch an elevated process without incurring a UAC prompt, but that's expected because Task Manager is on the list of programs which are allowed to elevate without a prompt. Of course, once you get to Task Manager, you can use that to launch other programs, but that's also to be expected, because that's one of the purposes of Task Manager.

The question then is whether there is a security vulnerability. To do that, we need to answer a few questions.

First, who is the attacker?

The attacker is presumably some malware running un-elevated which is trying to get itself elevated.

Who is the victim?

The victim is the user who has gotten tricked into running Task Manager, elevating it, and running the malware elevated.

But wait a second, is that really a valid victim? If you presuppose a victim who will follow the instructions of malware, then you don't need Task Manager. The malware can tell the victim, "Okay, run this program, and when it asks for permission, say Yes."

Okay, so maybe that's not the victim. Maybe the victim is a user whose account has been compromised by malware (e.g., by exploiting a bug elsewhere in the system), and now the malware is trying to use that as a foothold to auto-elevate itself.

In that scenario, the malware would programmatically launch Task Manager, programmatically click the "Show all processes" button, programmatically open the Run dialog, programmatically check the "Create this task with administrator privileges", programmtically fill in the program name, and programmatically click the OK button.

However, this scenario fails because the malware will be able to get as far as programmtically clicking the "Show all processes", and then all future options will be blocked by User Interface Privilege Isolation (UIPI), which prevents unelevated programs (like the malware) from programmatically driving the UI of elevated programs (like the elevated Task Manager).

In order for the malware to be able programmatically drive the UI of the elevated Task Manager, it must itself already be elevated, in which case it is already on the other side of the airtight hatchway.

Creating an object on the other side of the airtight hatchway is not in and of itself a security vulnerability. You also have to evaluate what you can do with that object. If the object can cause problems by its mere presence, or if you have control over the object and can cause it to create problem, then you have an issue. But if the object's mere existing is not problematic, and you have no control over the object, then you haven't gained anything. You may have annoyed the user (who now has to close that extra copy of Task Manager), but that's about it.

We never did get any details from the finder as to what those "wide-ranging security implications" are. The finder merely said, "This is a trivial UAC bypass."

Raymond Chen

Follow