

# Re: Windows XP Task Scheduler Local Privilege Escalation (Advisory)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-06/msg00319.html>

---

- *From:* "Elijah Kagan" <[degeneracypressure@xxxxxxxxx](mailto:degeneracypressure@xxxxxxxxx)>
  - *Date:* Mon, 12 Jun 2006 12:37:26 -0800
- 

From the article:

"Access to the at command varies, on some installations of Windows, even the Guest account can access it, on others it's limited to Administrator accounts."

But it's limited to members of the Administrators group by default. Anyone who is an administrator can make their system insecure by degrading the permissions to make them less restrictive than the vendor intended them to be. On any operating system, built on any security model, ever.

On a system where the administrator either knows what he/she is doing, or doesn't mess with things that he/she doesn't understand, this does not appear to be exploitable. And no security model can combat an incompetent administrator. Consequently, this does not appear to be a real vulnerability—unless you are saying that there is a bug in Windows that causes it to sometimes be installed, out of the box, with the guest user able to use the at command? (That would certainly merit an advisory, if true, but the paper focuses on how to use the at command, i.e., on what to do \*once\* you have obtained SYSTEM access. Can you give more detailed information about cases where non-administrative users are able to use the at command?)

I also think that it is misleading to say that SYSTEM can do things that an administrator can't, since any administrator can execute code as SYSTEM by installing a service to run as SYSTEM. Even if the task scheduler is disabled, someone with administrative privileges can still install system services. All the behavior that the article describes seems to be by design and none of it seems to constitute a security threat. Am I wrong?

By the way, on a related note, if the goal is to obtain a SYSTEM desktop for administrative purposes, a more elegant way to do it is to install a service that runs cmd.exe as SYSETM (using Microsoft's instsrv.exe and srvany.exe utilities, search MS Knowledge Base for more info), and then quit explorer.exe and related applications and

Re: Windows XP Task Scheduler Local Privilege Escalation (Advisory)

launch explorer.exe from the command prompt. (Or if you are running Server 2003, I think you can actually run programs as SYSTEM with RunAs.) This is essentially the same as the method described in the article, but it doesn't use the task scheduler for a purpose not relating to the scheduling of tasks, and works even if the task scheduler is disabled or run with reduced privileges.

-Elijah

On 6/11/06, zipk0der wrote:

-----  
= Advisory: Windows XP Task Scheduler Local Privilege Escalation  
=  
= Author: Daniel Hückmann (zipk0der) zipk0der@xxxxxxxxxxxxxxxxxxxxxx  
=  
= Released at: <http://www.pandora-security.com>  
=  
-----  
-----

1. Overview.

In Windows XP, the task scheduler service runs as "SYSTEM" (local service); this is akin to running cron as root. Any processes spawned by the task scheduler inherit "SYSTEM" permissions. Using command line tools, we can kill the Windows desktop (explorer.exe) and restart it running under "SYSTEM". Once running under "SYSTEM" we have full control of the machine, and can do things even Administrators can't. Also included is a recommended fix. Read the full paper at the link below.

-----  
Direct link to the original paper discussing this issue in detail...  
<http://www.pandora-security.com/forum/viewtopic.php?t=2093>  
-----

Sincerely,

Daniel Hückmann – R&D Director, Pandora Security