

## Re: The Kernal Is A Huge Security Whole In Windows

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-07/0690.html>

---

*From:* CHANGE USERNAME TO westes (~~DELETE\_westes\_at\_earthbroadcast.com~~)

*Date:* 07/15/04

Date: Thu, 15 Jul 2004 11:06:48 -0700

Regarding the dll cache, I have always wondered how does that get updated as you apply various service packs? Does Microsoft patch the dllcache at the same time? Should we put file security on that cache so that only administrators or system can access it?

The easiest way to exploit the security hole I am discussing is obviously the device driver. Putting off security responsibilities on the device driver writer is ridiculous, I'm sorry. You want to make the virus writer responsible for making his device driver secure? :)

```
--
Will
westes AT earthbroadcast.com
"Miha Pihler" <miha-news@atlantis.si> wrote in message
news:eWHs5LpaEHA.3596@tk2msftngp13.phx.gbl...
> Hi,
>
> critical system files are digitally signed and system checks for this
> signature. If you replace these files with new one that is not digitally
> signed system will restore it from e.g. dllcache
> (%systemroot%/system32/dllcache). If it cannot restore it it will ask for
> installation CD. Same thing happens if you change anything in any of these
> files -- you invalidate digital signature.
>
> You can check digital signatures on files by running "sigverif"...
>
> Also all patches and all service packs are digitally signed.
>
> I can't say that for system drivers, but that's up on vendors... You can
see
> amount of processor used by Kernel if you open Task Manager and click on
> Performance Tab > View > Show Kernel Times. You can also check some
> additional settings by clicking on Processes Tab > View > Select Columns.
>
> I hope this helps,
>
> Mike
>
> "CHANGE USERNAME TO westes" <DELETE_westes@earthbroadcast.com> wrote in
> message news:eflHw7oaEHA.2840@TK2MSFTNGP11.phx.gbl...
> > I'm starting to believe that the largest, and most dangerous, security
> hole
```

## microsoft.public.win2000.security: Re: The Kernal Is A Huge Security Whole In Windows

> > in Windows 2000 is the kernel itself. All a virus needs to do is  
> replace  
> > a key system file that will load into the kernel, or alternately install  
> as  
> > a device driver, and it can hide its behavior to the system. As far  
as  
> I  
> > can tell, there are no utilities that let me see how much CPU, disk, or  
> > network activity is performed by any component of the Windows 2000  
kernel.  
> >  
> > On one of my user's machines, her CPU goes to 100% as soon as she starts  
> up.  
> > We have stopped every single service and application on her machine, and  
> it  
> > doesn't change anything. Is this a virus? Is it a badly written  
device  
> > driver? Is some hardware generating interrupts that overwhelm the  
device  
> > driver? How can we know?  
> >  
> > As far as I can tell, there is nothing left to do here but re-install,  
> which  
> > risks that the entire sequence may happen yet again. If Microsoft  
> values  
> > security, this is a huge back door that they cannot allow to remain.  
> >  
> > --  
> > Will  
> > westes AT earthbroadcast.com  
> >  
> >  
>  
>