

Re: CIS Security Baseline

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-08/4768.html>

From: Leon (L.pholi@secureinteractive.com)

Date: 08/05/02

From: "Leon" <l.pholi@secureinteractive.com>

Date: Mon, 5 Aug 2002 12:39:09 +1000

Hey Matt,

That was exactly it. Thanks very much for your help, will let CIS know of this issue.

Leon

"Matt Scarborough" <vexversa@verizon.net> wrote in message
news:ht1lku05plvumpi2d1vab58g10a1lqfufs@msnews.microsoft.com...

> *I believe The Center for Internet Security template*

>

> ; *Template Name: Win2kProGold_R1.2.inf*

> ; *Template Version: R1.2*

> ; *Date Created: 2002-05-13*

> ; *Date Last Modified: 2002-06-13*

>

> *has created an endless loop from which you cannot escape.*

>

> *WFP by default protects all Microsoft provided DLL, EXE, OCX, and SYS files from*

> *installation media. However, all DLL, EXE, OCX, and SYS files are not installed to the*

> *hard disk for every machine. And some files may be removed from the machine or the DLL*

> *or Driver Caches during subsequent software, hardware, or hotfix installations. Even*

> *Microsoft has made mistakes with HOTFIX.INF files that fail to place updated files in*

> *the appropriate file caches. This can leave us with an entry for WFP to protect files*

> *that do not exist where WFP believes they should exist.*

>

> *The preceding condition can exist without significant trouble until we ask System File*

> *Checker to repopulate the %Systemroot%\system32\dllcache. Often the condition is not*

- > *discovered until we run for example*
- > *SFC /SCANNOW or SFC /SCANBOOT from the command line.*
- >
- > *Enter the Center for Internet Security template which sets these Registry entries*
- >
- > *HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\Sfcscan=4,1*
- > *HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\Sfcdisable=4,4*
- > *HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\Sfcshowprogress=4,0*
- >
- > *Those cause SFC to run at every boot and disable user interaction, i.e., disable the*
- > *pop-ups that tell you what is going on.*
- >
- > *Now the real gotcha! The CIS template also sets the following Registry entry*
- > *HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\AllocateCDRoms=1,1*
- >
- > *That Registry entry allows only the currently logged on user to access the CD-ROM.*
- > *SFC's parent process is Winlogon, running as LocalSystem. As such, without additional*
- > *code, SFC does not have rights to access the CD-ROM (where your missing files are*
- > *located.) And since the user interaction is disabled, you never know why.*
- >
- > *What I would do to fix this is*
- > *A) Ensure HKLM\Software\Microsoft\Windows\CurrentVersion\Setup*
- > *SourcePath=D:*
- > *points to the correct path of your installation media.*
- > *B) Change the template to*
- > *HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\Sfcscan=4,1*
- > *HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\Sfcdisable=4,0*
- > *HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\Sfcshowprogress=4,1*
- > *HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\AllocateCDRoms=1,0*
- > *and reload the template.*
- > *C) Reboot*
- > *D) Contact the The Center for Internet Security for support on this issue and guidance*
- > *in changing the settings.*
- >
- > *Matt Scarborough 2002-08-02*
- >
- > *On Wed, 31 Jul 2002 15:15:16 +1000, Leon wrote*
- > *<OmM8iEFOCHA.2532@tkmsftngp13>*
- > *> Hi,*
- > *>*

> > *I have been trialing the recently released Center for Internet Security
> > Win2k Gold (Level II) template on a few Win 2k Pro machines, and am
quite
> > happy with the majority of the default configurations. However there is
one
> > re-occurring event log message at every start up in the application log,
only
> > after the template is installed:
> >
> > Source: Windows File Protection
> >
> > Event ID: 64021
> >
> > Type: Information
> >
> > The system file c:\winnt\(\path)\(xxxxxx).dll could not be copied into
the
> > DLL cache. The specific error code is 0x000004c7 [The operation was
canceled
> > by the user.
> >
> > J. This file is necessary to maintain system stability.
> >
> > This error repeats many times at startup on all systems tested. The only
> > known cause of this previously was an issue with Service Pack 1, which
was
> > resolved in Service Pack 2. Microsoft stated at the time that this issue
was
> > not anything to be concerned with.
> >
> > Is there anyway of fixing it if it is an issue, or stopping the messages
if
> > it isn't?
> >
> > Or am I the only one who has come across this???*