

## Re: CIS Security Baseline

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-08/4847.html>

---

**From:** Matt Scarborough ([vexversa@verizon.net](mailto:vexversa@verizon.net))

**Date:** 08/06/02

From: Matt Scarborough <[vexversa@verizon.net](mailto:vexversa@verizon.net)>

Date: Tue, 06 Aug 2002 18:51:52 +0000

On Mon, 5 Aug 2002 13:05:45 +1000, Leon wrote

<#gV6ezCPCHA.2520@tkmsftngp08>

> *Just an additional note to this,*

>

> *While this did stop the errors, I found SFC very processor intensive for a*  
> *significant time at startup, and it would also prompt for the CD at EACH*  
> *startup, even when nothing had changed, so I turned off SFC totally by*  
> *setting Sfcscan to 4,0. Much better!!*

Hi Leon,

There are significant reasons why some choose to not enable SFC at every boot. You encountered a few yourself. Be sure to contrast the NIST templates with what you have.

[http://csrc.nist.gov/itsec/guidance\\_W2Kpro.html](http://csrc.nist.gov/itsec/guidance_W2Kpro.html)

The NIST templates themselves are documented and have an MS look and feel.

In limited scenarios, without Administrative intervention during implementation, applying these consensus templates can actually afford an advantage to a malicious hacker. But the broader scope encompassed by the consensus template \*I suppose is for improving neglected machines' security posture. So in general, those are better off using the template than not. Esoteric vulnerabilities are the expected outcome of non-secure-by-default installations mitigated by automated lockdown tools.

The biggest problem I see is a failure for some to remember the Security Configuration Editor tool and templates were designed to be used and applied incrementally to clean systems. SCE templates should \*not\* simply be ripped from the web during the waning years of an OS (Windows 2000 Service Pack 3) and be applied in a misguided effort to pro-actively secure live systems. At that point in time security conscious clients' needs can probably be better served by rolling out XP. If it took several years to get around to securing their Windows 2000 machines, the security built-in to XP would serve them well.

The second troubling aspect in this seeming mad rush to keep the Internet safe from Windows, is the lack of attention paid to including explicit, default settings in the template. When no setting of

...\Winlogon\AllocateCDRoms=n,n

for example is included in these consensus templates we are left to rely on (a) that some previous template applied the default value of `allocatcdroms=1,0` or (b) that no previously template was applied.

In Leon's case the value was changed (perhaps by the application of `CIS-Win2K-Level-I-v1.1.7.inf`) and resulted in the problem of an inaccessible CD-ROM drive (due to an existing setting of `allocatcdroms=1,1` that was not cleared) by SFC at boot. Surely had CIS intended the value to be `allocatcdroms=1,1` they would have included it (?)

Again, in an incremental scenario, generic Internet connected Win2k boxes should require drives are formatted NTFS \*prior\* to OS installation to ensure "setup security.inf" rights and permissions are applied as designed. Further, incremental application ensures the application of appropriate permissions in `basicwk.inf`.

```
;-----  
;x86 Boot Files  
;-----  
and  
;-----  
;System Drive (\\)  
;-----  
and  
;Ignored Dirs do not exist when security applied during setup.
```

This documented step-by-step procedure of incremental template installation (`secedit [enter]` opens the Help topic) is often missed by security researchers on NTBugtraq.

FWIW, checking machine patch status with `HFNetChk -v -z`, and checking the system catalog with `QFECheck`, are both better methods IMHO than enabling automated System File Checking such as an SCE template that enforces "SFC /scanboot." We try to place a slip streamed version of SP3 installation source files in a location accessible to the SFC process when it runs, although I'm not sure Microsoft supports that.

QFECheck

<http://support.microsoft.com/support/kb/articles/Q282/7/84.ASP>

SFC

<http://support.microsoft.com/support/kb/articles/Q222/4/71.ASP>

WFP

<http://support.microsoft.com/support/kb/articles/q222/1/93.asp>

Heads up although the new XCACLS may fix this(?)

<http://support.microsoft.com/support/kb/articles/Q321/4/70.asp>

Matt Scarborough 2002-08-06

```
> "Matt Scarborough" <vexversa@verizon.net> wrote in message  
> news:ht1lku05plvumpi2d1vab58g10a11qfufs@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\dlldata. 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\Sfcsan=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\Sfcsan=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@ikmsftngp13>*  
> > > *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.*  
> > >  
> > > *] 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???*  
> > >  
> >  
>