
Safe'nSec - Insecure File execution and Auto-startup

Ref : TZO-062006-SafenSec
Author : Thierry Zoller
WWW : http://secdev.zoller.lu
Article : http://secdev.zoller.lu/research/safensec.htm

I. Background

"Safe'n'Sec is complex data and user applications protection against threats and vulnerabilities for individual PC as well as workstations in corporate networks. The program uses proactive technology based on activity analysis in user PC."

II. Description

Vulnerable versions :
- Safe'nSec Personla and Antispyware v2.0 and older
- Probably the other versions of Safe'nSec

Multiple Insecure File execution and Autostart handling.

During Startup,
snsmcon.exe spawns the GUI process named safensec.exe through the use of CreateProcess() . By doing so it omits to set the variable'lpApplicationName'

and further omits to quote the path in the variable "lpCommandLine" Ref [1]

This results in c:\program.bat|exe|com being called prior to Sr_GUI.exe and allows
automatic startup of a potentially rogue application. In particular one could imagine a scenario where it is possible to escalate rights using this (as they are inherited from snsmcon.exe).

During Autostartup
Safe'nSec omits the quotes around the path to the executable and as such may spawn a rogue application instead of the appropriate Starforce application.

During Installation:
During installion a routine spawns a process and omits the quotes around the path, thus executing c:\program.exe (here calc.exe)

III. Summary

Vendor contact : 15/02/2006
Vendor Response : None

Vendor Response :
None

[1] http://lists.grok.org.uk/pipermail/full-disclosure/2005-November/038789.html
[2] Only a real issue in Windows 2000, WinXP restricted users don't have the right to write to c:\