

Free Fixer Log (posted 10.28)

Posted by chartaine - 2008/10/29 05:37

FreeFixer v0.27 log

<http://www.freefixer.com/>

Operating system: Windows Vista Service Pack 1

Log dated 2008-10-28 21:34

Namespace service providers (6 whitelisted)

{B600E6E9-553B-4A19-8696-335E5C896153} - C:\Program Files\Bonjour\mdnsNSP.dll

Browser Helper Objects

{02478D38-C3F9-4efb-9B51-7695ECA05670}, &Yahoo! Toolbar Helper, C:\Program Files\Yahoo!\Companion\Installs\cpn\yt.dll

{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}, Adobe PDF Reader Link Helper, C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll

{377C180E-6F0E-4D4C-980F-F45BD3D40CF4}, McAfee Phishing Filter, c:\PROGRA~1\mcafee\msk\mcapbho.dll

{72853161-30C5-4D22-B7F9-0BBC1D38A37E}, Groove GFS Browser Helper,

C:\PROGRA~1\MICROS~2\Office12\GRA8E1~1.DLL

{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}, SSVHelper Class, C:\Program Files\Java\jre1.6.0_07\bin\ssv.dll

{7DB2D5A0-7241-4E79-B68D-6309F01C5231}, scriptproxy, C:\Program Files\McAfee\VirusScan\scriptsn.dll

{83A2F9B1-01A2-4AA5-87D1-45B6B8505E96}, ShowBarObj Class, C:\Acer\Empowering

Technology\eDataSecurity\x86\ActiveToolBand.dll

{B164E929-A1B6-4A06-B104-2CD0E90A88FF}, McAfee SiteAdvisor BHO, c:\PROGRA~1\mcafee\SITEAD~1\mcieplg.dll

Internet Explorer toolbars

HKLM\..\Toolbar\{EF99BD32-C1FB-11D2-892F-0090271D4F88} - Yahoo! Toolbar - C:\Program Files\Yahoo!\Companion\Installs\cpn\yt.dll

HKLM\..\Toolbar\{5CBE3B7C-1E47-477e-A7DD-396DB0476E29} - Acer eDataSecurity Management - C:\Acer\Empowering Technology\eDataSecurity\x86\edStoolbar.dll

HKLM\..\Toolbar\{0EBBBE48-BAD4-4B4C-8E5A-516ABECAE064} - McAfee SiteAdvisor Toolbar - c:\PROGRA~1\mcafee\SITEAD~1\mcieplg.dll

Basic Internet Explorer settings

HKCU\..\Main, Start Page = <http://en.us.acer.yahoo.com/>

HKLM\..\Main, Start Page = http://en.us.acer.yahoo.com

HKCU\..\Main, Search Page = <http://go.microsoft.com/fwlink/?LinkId=54896>

HKLM\..\Main, Search Page = <http://go.microsoft.com/fwlink/?LinkId=54896>

HKLM\..\Main, Default_Page_URL = <http://en.us.acer.yahoo.com>

HKLM\..\Main, Default_Search_URL = <http://go.microsoft.com/fwlink/?LinkId=54896>

Registry Startups (1 whitelisted)

HKLM\..\Run, IAAnotif = "C:\Program Files\Intel\Intel Matrix Storage Manager\laanotif.exe"

HKLM\..\Run, RtHDVCpl = RtHDVCpl.exe

HKLM\..\Run, SynTPStart = C:\Program Files\Synaptics\SynTP\SynTPStart.exe

HKLM\..\Run, mcagent_exe = C:\Program Files\McAfee.com\Agent\mcagent.exe /runkey

HKLM\..\Run, IgfxTray = C:\Windows\system32\igfxtray.exe

HKLM\..\Run, HotKeysCmds = C:\Windows\system32\hkcmd.exe

HKLM\..\Run, Persistence = C:\Windows\system32\igfxpers.exe

HKLM\..\Run, PLFSetL = C:\Windows\PLFSetL.exe

HKLM\..\Run, PLFSetI = C:\Windows\PLFSetI.exe

HKLM\..\Run, RemoteControl = "C:\Program Files\CyberLink\PowerDVD\PDVDServ.exe"

HKLM\..\Run, LanguageShortcut = "C:\Program Files\CyberLink\PowerDVD\Language\Language.exe"

HKLM\..\Run, eDataSecurity Loader = C:\Acer\Empowering Technology\eDataSecurity\x86\eDSloader.exe

HKLM\..\Run, LManager = C:\PROGRA~1\LAUNCH~1\LManager.exe

HKLM\..\Run, eRecoveryService = (file is missing)

HKLM\..\Run, Acer Assist Launcher = C:\Program Files\Acer\Acer Assist\launcher.exe

HKLM\..\Run, Acer Product Registration = "C:\Program Files\Acer\Acer Registration\ACE1.exe" /startup

HKLM\..\Run, SunJavaUpdateSched = "C:\Program Files\Java\jre1.6.0_07\bin\jusched.exe"

HKLM\..\Run, GrooveMonitor = "C:\Program Files\Microsoft Office\Office12\GrooveMonitor.exe"

HKLM\..\Run, QuickTime Task = "C:\Program Files\QuickTime\QTTask.exe" -atboottime

HKLM\..\Run, Zune Launcher = "C:\Program Files\Zune\ZuneLauncher.exe"

HKLM\..\Run, AppleSyncNotifier = C:\Program Files\Common Files\Apple\Mobile Device Support\bin\AppleSyncNotifier.exe

HKLM\...\Run, iTunesHelper = "C:\Program Files\iTunes\iTunesHelper.exe"
HKLM\...\Run, Adobe Reader Speed Launcher = "C:\Program Files\Adobe\Reader 8.0\Reader\Reader_sl.exe"
HKCU\...\Run, AlcoholAutomount = "C:\Program Files\Alcohol Soft\Alcohol 120\axcmd.exe" /automount
HKCU\...\Run, BitTorrent = "D:\Program Files\BitTorrent\bittorrent.exe" --force_start_minimized

Autostart shortcuts

OneNote 2007 Screen Clipper and Launcher.lnk, Screen Clipper (Windows+S) and Launcher (Windows+N) for Microsoft Office OneNote., C:\Program Files\Microsoft Office\Office12\ONENOTEM.EXE

HOSTS file

75.125.165.202 financialtopic.com
64.14.244.60 thefestivals.com
208.254.26.132 clickscasino.net
208.254.26.132 polarcafe.com
64.14.244.60 usaplasticsurgeons.com
64.14.244.60 gallerycities.com
208.254.26.132 supportingourtroops.com
208.254.26.132 lehmaninbev.com
208.254.26.132 escapefromreality.com
64.14.244.60 luxuryglobal.com
64.34.46.60 LouisianaVoices.com

Processes (38 whitelisted)

(file is missing)

OpenProcess failed while opening process # 1288 to get its full path. Process filename: audiodg.exe. System error message: Access is denied.

C:\Program Files\Lavasoft\Ad-Aware\aaawservice.exe
C:\Program Files\Intel\Intel Matrix Storage Manager\IAAnotif.exe
C:\Windows\RtHDVCpl.exe
C:\Program Files\Synaptics\SynTP\SynTPStart.exe
C:\Program Files\McAfee.com\Agent\mcagent.exe
C:\Windows\System32\hkcmd.exe
C:\Windows\System32\igfxpers.exe
C:\Windows\PLFSetL.exe
C:\Windows\PLFSetI.exe
C:\Program Files\CyberLink\PowerDVD\PDVDServ.exe
C:\Acer\Empowering Technology\DataSecurity\x86\EDSLoader.exe
C:\Users\Matt\AppData\Local\Temp\RtkBtMnt.exe
C:\Windows\System32\afisicx.exe
C:\Program Files\Common Files\Apple\Mobile Device Support\bin\AppleMobileDeviceService.exe
C:\Program Files\Bonjour\mDNSResponder.exe
C:\Acer\Empowering Technology\DataSecurity\x86\EDSService.exe
C:\Acer\Empowering Technology\Lock\Service\LockServ.exe
C:\Acer\Empowering Technology\Net\Net Service.exe
C:\Program Files\Intel\Intel Matrix Storage Manager\IAANTmon.exe
C:\Program Files\Common Files\LightScribe\LSSrvc.exe
C:\Program Files\McAfee\SiteAdvisor\McSACore.exe
C:\PROGRA~1\COMMON~1\McAfee\McProxy\McProxy.exe
C:\PROGRA~1\McAfee\VIRUSS~1\Mcshield.exe
C:\Acer\Mobility Center\MobilityService.exe
C:\Program Files\McAfee\MPF\MpfSrv.exe
C:\Program Files\McAfee\MSK\msksrver.exe
C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.exe
C:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\Binn\sqlservr.exe
C:\Windows\System32\noytcyr.exe
C:\Windows\System32\perfs.exe
C:\Windows\System32\roytctm.exe
C:\Windows\System32\solewxt.exe
C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe
C:\Windows\System32\tdydowkc.exe
C:\Windows\System32\wsldoekd.exe
C:\Windows\System32\drivers\XAudio.exe
C:\Acer\Empowering Technology\Recovery\RecoveryService.exe
C:\Acer\Empowering Technology\Settings\Service\capuser.exe

C:\Acer\Empowering Technology\Power\PowerSvc.exe
C:\PROGRA~1\McAfee\MSC\mcmcsvc.exe
C:\Program Files\Launch Manager\LManager.exe
C:\Program Files\Synaptics\SynTP\SynTPEnh.exe
C:\Program Files\Java\jre1.6.0_07\bin\jusched.exe
C:\Program Files\Microsoft Office\Office12\GrooveMonitor.exe
C:\Program Files\Zune\ZuneLauncher.exe
C:\Program Files\iTunes\iTunesHelper.exe
C:\Windows\System32\igfxext.exe
C:\Windows\System32\igfxsrvc.exe
C:\Program Files\iPod\bin\iPodService.exe
C:\PROGRA~1\McAfee\VIRUSS~1\mcysmon.exe
C:\Program Files\Common Files\McAfee\MNA\McNASvc.exe
C:\Program Files\McAfee\MSC\mcuimgr.exe
C:\Windows\System32\igfxsrvc.exe
C:\Windows\System32\tpsxyd.sys
C:\Windows\System32\mabidwe.exe
C:\Windows\System32\soxpeca.exe
C:\Windows\System32\Macromed\Flash\FlashUtil9f.exe
C:\Program Files\McAfee\VirusScan\mcsvshld.exe
C:\Windows\System32\udxfytw.sys
D:\Program Files\FreeFixer\freefixer.exe

Application modules (44 whitelisted)

C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.6001.18000_none_886786f450a74a05\COMCTL32.dll
C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6001.18000_none_5cdbaa5a083979cc\comctl32.dll
C:\Program Files\McAfee\SiteAdvisor\saHook.dll

Services (61 whitelisted)

aawservice, Lavasoft Ad-Aware Service, c:\program files\lavasoft\ad-aware\laawservice.exe
afisicx, afisicx Service, c:\windows\system32\afisicx.exe
Apple Mobile Device, Apple Mobile Device, c:\program files\common files\apple\mobile device
support\bin\applemobiledeviceservice.exe
Bonjour Service, Bonjour Service, c:\program files\bonjour\mdnsresponder.exe
eDataSecurity Service, eDataSecurity Service, c:\acer\empowering technology\edatasecurity\x86\edservice.exe
eLockService, eLock Service, c:\acer\empowering technology\elock\service\elockserv.exe
eNet Service, eNet Service, c:\acer\empowering technology\enet\enet service.exe
eRecoveryService, eRecovery Service, c:\acer\empowering technology\erecovery\erecoveryservice.exe
eSettingsService, eSettings Service, c:\acer\empowering technology\esettings\service\capuser.exe
IAANTMON, Intel(R) Matrix Storage Event Monitor, c:\program files\intel\intel matrix storage manager\iaantmon.exe
LightScribeService, LightScribeService Direct Disc Labeling Service, c:\program files\common files\lightscribe\lssrv.exe
mabidwe, mabidwe Service, c:\windows\system32\mabidwe.exe
macidwe, macidwe Service, c:\windows\system32\macidwe.exe (file is missing)
McAfee SiteAdvisor Service, McAfee SiteAdvisor Service, c:\program files\mcafee\siteadvisor\mcsacore.exe
mcmcsvc, McAfee Services, c:\progra~1\mcafee\msc\mcmcsvc.exe
McNASvc, McAfee Network Agent, c:\progra~1\common~1\mcafee\mna\mcnasvc.exe
McProxy, McAfee Proxy Service, c:\progra~1\common~1\mcafee\mcproxy\mcproxy.exe
McShield, McAfee Real-time Scanner, c:\progra~1\mcafee\virus~1\mcshield.exe
MobilityService, MobilityService, c:\acer\mobility center\mobilityservice.exe
MpfService, McAfee Personal Firewall Service, c:\program files\mcafee\mpf\mpfsrv.exe
MSK80Service, McAfee Anti-Spam Service, c:\program files\mcafee\msk\msksrver.exe
MSSQL\$MSSMLBIZ, SQL Server (MSSMLBIZ), c:\program files\microsoft sql server\mssql.1\mssql\binn\sqlservr.exe
MSSQL\$SQLEXPRESS, SQL Server (SQLEXPRESS), c:\program files\microsoft sql
server\mssql10.sqlexpress\mssql\binn\sqlservr.exe
noxtcyr, noxtcyr Manages messages, c:\windows\system32\noxtcyr.exe (file is missing)
noytcyr, noytcyr Service, c:\windows\system32\noytcyr.exe
perfmons, perfmons, c:\windows\system32\perfs.exe
roytctm, roytctm Service, c:\windows\system32\roytctm.exe
sobicyt, sobicyt, c:\windows\system32\sobicyt.exe (file is missing)
solewxtte, solewxtte Service, c:\windows\system32\solewxtte.exe
soxpeca, soxpeca Service, c:\windows\system32\soxpeca.exe
SQLWriter, SQL Server VSS Writer, c:\program files\microsoft sql server\90\shared\sqlwriter.exe
tdydowkc, tdydowkc Service, c:\windows\system32\tdydowkc.exe

WMIService, ePower Service, c:\acer\empowering technology\epower\epowersvc.exe
wsldoekd, wsldoekd Service, c:\windows\system32\wsldoekd.exe
XAudioService, XAudioService, c:\windows\system32\drivers\xaudio.exe

Drivers (39 whitelisted)

crcdisk, Crcdisk Filter Driver, C:\Windows\system32\drivers\crcdisk.sys
iaStor, Intel AHCI Controller, C:\Windows\system32\drivers\iaStor.sys
int15, int15, c:\windows\system32\drivers\int15.sys
intelide, , C:\Windows\system32\drivers\intelide.sys
mdmxsdk, , C:\Windows\system32\drivers\mdmxsdk.sys
mfehdk, McAfee Inc. mfehdk, C:\Windows\system32\drivers\mfehdk.sys
MPFP, MPFP, C:\Windows\system32\drivers\mpfp.sys
Parvdm, , C:\Windows\system32\drivers\parvdm.sys
PSDNServ, PSDNServ, C:\Windows\system32\drivers\psdnserv.sys
psvdisk, PSDVdisk, C:\Windows\system32\drivers\psvdisk.sys
sptd, , C:\Windows\system32\drivers\sptd.sys

An error occurred when trying to open the file for reading.

Filename: 'C:\Windows\system32\drivers\sptd.sys'.

Current Working Directory: 'D:\Program Files\FreeFixer\'.
System error message: The process cannot access the file because it is being used by another process.

C++ exception: ios_base::failbit set

sxuftp, SXUFTP Driver, C:\Windows\system32\drivers\sxuftp.sys

XAudio, , C:\Windows\system32\drivers\xaudio.sys

=====