Collecting Mini-Dumps for User Crashes

## 11/4/2012 - BackTrak

# Overview – If you can reproduce it, you can fix it!

There will be times when a user is experiencing issues with their Allegiance installation. These issues can range from .Net based security client issues to the Allegiance client itself. When the issue is the Allegiance client it can be very difficult to determine where the issue is coming from within the Allegiance C++ code base. To help determine the cause of the issue, a Microsoft program called ProcDump can be registered on the user’s computer as a “Just In Time Debugger”. This will enable Windows to intercept the error from Allegiance and then use ProcDump to create a Mini-Dump of the entire Allegiance process included the memory and call stack at the time of error. This can then be loaded back into Visual Studio and the entire user’s application context will be available. Visual Studio will be stopped at the exact location the error occurred and most of the memory / call stack details will be available. With this information, finding the cause of the issue becomes elementary.

# Have the user set up their machine for debugging

1. Request the user download <http://acss.alleg.net/downloads/DebugSupport.zip>. This archive will contain ProcDump and the .PDB files for Allegiance.exe and AGC.dll. These .PDB files must match the current build or the Allegiance.exe client the user is running. Because the .PDB files are quite large, they should not be added to the standard Allegiance Auto Update system.
2. Have the user extract DebugSuport.zi p to their local hard drive (c:\DebugSupport).
3. Have the user run: c:\DebugSupport\CrashDumpActivate.bat as Administrator.
4. Have the user reproduce the crash.
5. When Allegiance.exe crashes, a dialog window will appear. Have the user select “Debug” from the options list.
6. A crash dump file will appear in c:\DebugSupport\minidump.dmp.
7. Have the user send you the minidump.dmp file.
8. You are now ready to debug the crash.
9. The user can remove the ProcDump debugger hook and restore any previous debugger hooks by running c:\DebugSupport\CrashDumpDeactivate.bat

# Using the mini-dump to debug the issue

1. Ensure that you have Visual Studio 2010, and that you have the debug symbols setup to download from Microsoft’s Symbol Server. See <http://msdn.microsoft.com/en-us/library/b8ttk8zy%28v=vs.100%29.aspx>
2. Once you receive the mini-dump, place it anywhere on your local hard drive.
3. Get the build version of Allegiance that the user is running from SVN.
4. Get the Allegiance.pdb symbols file from <http://acss.alleg.net/downloads/AllegiancePDB.zip>
5. Open Allegiance.sln from the VS2010 source directory.
6. Next, from Visual Studio 2010, use File->Open and open the mini-dump file.
7. You will be prompted for symbols for Allegiance.exe. Browse to the Allegiance.pdb file from AllegiancePDB.zip.
8. Many things will load at this point. Once they are done, you will see a minidump file summary in VS2010. Click “Debug With Native Symbols Only”.
9. Visual Studio will break at the exact point of the crash on the user’s system. You may now proceed to debug.