

1 October 2008

By: Marius Oiaga, Technology News Editor

Windows
Microsoft

[Download Process Monitor 2.0 for Vista and XP](#)

Now with network tracing

At the start of September 2008, Microsoft Technical Fellow Mark Russinovich revealed that he was cooking a [major update for Process Monitor](#), one of the components of the Sysinternals suite. As of September 30, version 2.0 of Process Monitor became available for download. The [description of the tool](#) authored by Mark Russinovich and Bryce Cogswell reveals that Process Monitor 2.0 is designed to integrate seamlessly with both the 32-bit and 64-bit versions of Windows 2000 SP4 with Update Rollup 1, Windows XP SP2, Windows Server 2003 SP1, and Windows Vista.

"Process Monitor v2.0: this major update to Process Monitor adds real-time TCP and UDP monitoring to its existing process, thread, DLL, file system and registry monitoring. You can now see the TCP and UDP activity processes performed, including the operation (e.g. connect, send, receive), local and remote IP addresses and DNS names, and operation transfer lengths. On Windows Vista, Process Monitor also collects thread stacks for network operations," revealed [Curtis Metz](#), Program Manager, Microsoft Sysinternals.

Concomitantly with the new release of Process Monitor 2.0, the entire Sysinternals suite was update and is also available for download. Russinovich refreshed two additional utilitoes on top of Process Monitor 2.0, namely Sigcheck and Contig. "Sigcheck v1.54: this Sigcheck release fixes a bug in CSV output formatting. Contig v1.55: Contig now supports the -accepteula command-line switch," Metz added.

Via Process Monitor 2.0, users will be able to monitor in real time the file system of the Windows operating system along with the platform's registry and process/thread activity. Back in early September, Russinovich promised that Process Monitor would indeed evolve with the addition of new low-level capabilities, including a more intimate focus on memory usage, while at the same time delivering network tracing to the utility.

Process Monitor 2.0 is available for download [here](#).

The Sysinternals Suite is available for download [here](#).