



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: September 15, 2010.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Windows Print Spooler RPCStartDocPrinter Vulnerability (MS10-061,CVE-2010-2729).

Top Layer Products: IPS 5500 v4.X and higher.

Vulnerable Infrastructure: Microsoft Windows XP Service Pack 3, Windows XP Professional x64 Edition Service Pack 2, Windows Server 2003 Service Pack 2, Windows Server 2003 x64 Edition Service Pack 2, Windows Server 2003 with SP2 for Itanium-based Systems, Windows Vista Service Pack 1 and Windows Vista Service Pack 2, Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2, Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2, Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2, Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2, Windows 7 for 32-bit Systems, Windows 7 for x64-based Systems, Windows Server 2008 R2 for x64-based Systems, Windows Server 2008 R2 for Itanium-based Systems.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems

Advisory Impact: Prevention

Summary: The Microsoft Windows Print Spooler service manages the printing process on computers running Microsoft Windows. The service is started when the operating system starts; the tasks performed by the service include determining the correct printer driver, loading the driver, spooling function calls into a print job, scheduling print jobs, and passing the jobs to the print router. The reported Microsoft Windows Print Spooler vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user by sending a specially crafted print request to a vulnerable system that has a print spooler interface exposed over RPC.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2010-09-14-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft Windows Print Spooler RPCStartDocPrinter Vulnerability that will be applied to the “Recommended Client Protection” and “Recommended Server Protection” IPS Rule Sets.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-008005 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Windows infrastructure running Print Spooler services.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/ms10-061.msp

Relevant TLN Rules: tln-008005

Relevant TopResponse Protection Pack(s): 2010-09-14-01