Palo Alto Networks Discovers Critical Vulnerabilities in Windows Print Spooler and Remote Administration Protocol

August 14, 2012

Vulnerabilities Allow Attackers to Remotely Execute Code and Take Control of Systems

SANTA CLARA, Calif., Aug. 14, 2012 /PRNewswire/ -- Palo Alto Networks™ (NYSE: PANW), the network security company, today announced that its Threat Research Team was credited with identifying two critical vulnerabilities and one important vulnerability in the Remote Administration Protocol (RAP) and one critical vulnerability in the Windows Print Spooler service.

The discovered critical vulnerability in the Windows Print Spooler – CVE-2012-1851 – is a remote code execution vulnerability that could allow an attacker to run arbitrary code on a user's system with system privileges and take control of the affected system. This vulnerability is in Windows XP and Windows Server 2003 machines. This vulnerability will also result in a Denial of Service state in Windows Vista, Windows 7 and Windows Server 2008.

The discovered critical vulnerabilities in the Remote Administration Protocol – CVE-2012-1852 and CVE-2012-1853 – are heap and stack overflow vulnerabilities that could allow an attacker to remotely take control of the affected system. Both vulnerabilities are in Windows XP.

The discovered important Remote Administration Protocol vulnerability – CVE-2012-1850 – could allow an attacker who successfully exploited this vulnerability to cause a target application to stop responding. CVE-2012-1850 is in multiple versions of Windows and Windows Server.

The Palo Alto Networks Threat Research Team

The Palo Alto Networks Threat Research Team is active in the research community, aggressively pursuing both new vulnerability research and alleviation of all types of threats. The team has leveraged its expertise to uncover a string of critical and important vulnerabilities and has then worked with Microsoft to make sure users are protected.

SOURCE Palo Alto Networks

Mike Haro, Palo Alto Networks, +1-408-438-8628, mharo@paloaltonetworks.com