Microsoft Patch Tuesday: March 10th, 2009

Executive Summary

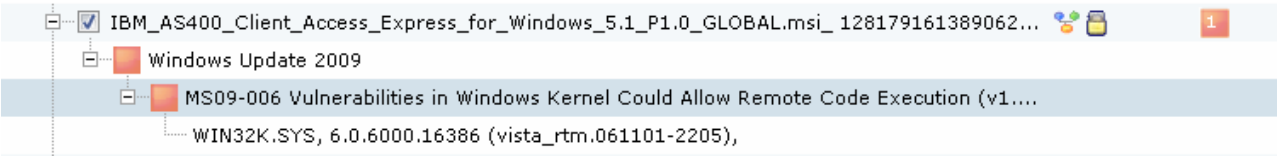
This month includes 3 patches, one rated Critical and the other rated as Important. These patches affect all operating systems from Windows 2000, XP through to VISTA and Windows 7 beta and will require all servers and desktops running these operating systems to be rebooted. The good news is that from an application compatibility perspective this is a minor update from Microsoft.

This will bring relief to IT departments after the February release.

Looking further at the March update, after loading the ChangeBase AOK application testing portfolio into a Patch Impact database, all three patches were tested for application level issues and in addition, application dependencies. None of three patches (MS09-006, MS09-007, and MS09-008) raised significant numbers of application level or dependency level issues with the AOK Application Test portfolio.

Given the very low numbers of issues, the ChangeBase AOK team recommends that these patches are rapidly deployed to a staging environment and then subsequently into Production. The ChangeBase AOK team recommends that with all changes to an environment basic UAT testing is performed on all business critical applications. However, for these three March Microsoft Security updates, only marginal build level testing should be required.

Here is a sample report extract from one of the few applications in the AOK ChangeBase Application Test Portfolio that raised a dependency level issue with the MS09-006 Security Update.



Testing Summary

MS09-006: Marginal Impact (both Package level and dependencies) detected across portfolio
MS09-007: Marginal Impact (both Package level and dependencies) detected across portfolio
MS09-008: Marginal Impact (both Package level and dependencies) detected across portfolio

Patch Name	Issues	% Affected	Reboot	Rating	RAG
Microsoft Security Bulletin MS09-006	27	<1%	YES	Critical	
Microsoft Security Bulletin MS09-007	7	<1%	YES	Important	
Microsoft Security Bulletin MS09-008	22	<1%	YES	Important	

Legend:

	Limited Issues Detected
	Potentially fixable application Impact
	Serious Compatibility Issue

Security Update Detailed Summary

MS09-006	**Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)**
Description	This security update resolves several privately reported vulnerabilities in the Windows kernel. The most serious vulnerability could allow remote code execution if a user viewed a specially crafted EMF or WMF image file from an affected system.
Payload	Win32k.sys
Impact	Remote Code Execution

MS09-007	**Vulnerability in SChannel Could Allow Spoofing (960225)**
Description	This security update resolves a privately reported vulnerability in the Secure Channel (SChannel) security package in Windows. The vulnerability could allow spoofing if an attacker gains access to the certificate used by the end user for authentication. Customers are only affected when the public key component of the certificate used for authentication has been obtained by the attacker through other means.
Payload	Schannel.dll
Impact	Spoofing

MS09-008	**Vulnerabilities in DNS and WINS Server Could Allow Spoofing (962238)**
Description	This security update resolves two privately reported vulnerabilities and two publicly disclosed vulnerabilities in Windows DNS server and Windows WINS server. These vulnerabilities could allow a remote attacker to redirect network traffic intended for systems on the Internet to the attacker's own systems.
Payload	Afd.sys, Dns.exe, Dnsperf.dll, Dnsperf.h, Dnsperf.ini, Msafd.dll, Sp3res.dll, Tcpip.sys
Impact	Spoofing

c. 800 applications were tested against these patches using the ChangeBASE ACL (Application Compatibility Lab)