Microsoft Patch Tuesday: February 11th, 2009

Executive Summary

This is a serious update from Microsoft for the February Security Update. This update includes two critical and two important updates – all of which require system restarts (both server and workstation platforms). The Microsoft Security Update MS09-002 should be treated with caution as a high proportion of applications in our portfolio had dependencies on these changes.

The message from the ChangeBASE team is that the Microsoft update MSO9-002 changes a large number of components and a very high proportion of applications are dependent on these changes. Organisations should seriously consider testing a good cross section of their application portfolio.

Testing Summary

- MS09-002: Severe Impact (both Package level and dependencies) detected across portfolio
- MS09-003: Marginal Impact (both Package level and dependencies) detected across portfolio
- MS09-004: Moderate Impact (both Package level and dependencies) detected across portfolio
- MS09-005: Moderate Impact (both Package level and dependencies) detected across portfolio

Patch Name	Matches	% Affected	Reboot	Rating	RAG
Microsoft Security Bulletin MS09-002	1762	91%	YES	Critical	
Microsoft Security Bulletin MS09-003	40	<1%	YES	Critical	
Microsoft Security Bulletin MS09-004	2904	<23%	YES	Important	
Microsoft Security Bulletin MS09-005	533	37%	YES	Important	

Legend:

	No Issues Detected
	Potentially fixable application Impact
	Serious Compatibility Issue

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

Security Update Detailed Summary

MS09-002	**Cumulative Security Update for Internet Explorer (961260)**
Description	This security update resolves two privately reported vulnerabilities. The vulnerabilities could allow remote code execution if a user views a specially crafted Web page using Internet Explorer. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. This update requires a restart.
Payload	Advpack.dll, Dxtmsft.dll, Dxtrans.dll, Extmgr.dll, Icardie.dll, Ie4uinit.exe, Ieakeng.dll, Ieaksie.dll, Ieakui.dll, Ieapfltr.dat, Ieapfltr.dll, Iedkcs32.dll, Ieframe.dll, Ieframe.dll.mui, Iernonce.dll, Iertutil.dll, Ieudinit.exe, Iexplore.exe, Inetcpl.cpl, Jsproxy.dll, Msfeeds.dll, Msfeedsbs.dll, Mshtml.dll, Mshtmled.dll, Msrating.dll, Mstime.dll, Occache.dll, Pngfilt.dll, Url.dll, Urlmon.dll, Webcheck.dll, Wininet.dll, Advpack.dll, Dxtmsft.dll, Dxtrans.dll, Extmgr.dll, Icardie.dll, Ie4uinit.exe, Ieakeng.dll, Ieaksie.dll, Ieakui.dll, Ieapfltr.dat, Ieapfltr.dll, Iedkcs32.dll, Ieframe.dll, Ieframe.dll.mui, Iernonce.dll, Iertutil.dll, Ieudinit.exe, Iexplore.exe, Inetcpl.cpl, Jsproxy.dll, Msfeeds.dll, Msfeedsbs.dll, Mshtml.dll, Mshtmled.dll, Msrating.dll, Mstime.dll, Occache.dll, Pngfilt.dll, Url.dll, Urlmon.dll, Webcheck.dll, Wininet.dll
Impact	Remote Code Execution

MS09-003	**Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution (959239)**
Description	This security update resolves two privately reported vulnerabilities in Microsoft Exchange Server. The first vulnerability could allow remote code execution if a specially crafted TNEF message is sent to a Microsoft Exchange Server. An attacker who successfully exploited this vulnerability could take complete control of the affected system with Exchange Server service account privileges. The second vulnerability could allow denial of service if a specially crafted MAPI command is sent to a Microsoft Exchange Server. An attacker who successfully exploited this vulnerability could cause the Microsoft Exchange System Attendant service and other services that use the EMSMDB32 provider to stop responding.
Payload	Cdo.dll, , Emsmdb32.dll, Emsmta.exe, Exhotfixuninst.dll, Exspmsg.dll, Mapi32.dll, Mdbmsg.dll, Store.exe, Exhotfix.cdd
Impact	Remote Code Execution

MS09-004	**Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420)**
Description	This security update resolves a privately reported vulnerability in Microsoft SQL Server. The vulnerability could allow remote code execution if untrusted users access an affected system or if a SQL injection attack occurs to an affected system. Systems with SQL Server 7.0 Service Pack 4, SQL Server 2005 Service Pack 3, and SQL Server 2008 are not affected by this issue.
Payload	Atl71.dll, Atxcore.dll, Atxcore.rll, Axscphst.dll, Axscphst.rll, Bcp.exe, Bcp.rll, Cldtcstp.exe, Cldtcstp.rll, Cmdwrap.exe, Cnfgsvr.exe, Cnvrem.dll, Cnvsvc.exe, Comnevnt.dll, Custtask.dll, Custtask.rll, Dbghelp.dll, Dbmslpcn.dll, Dbmslpcn.dll, Dbmsshrn.dll, Dbmsshrn.dll, Dbnetlib.dll, Dcomscm.exe, Distrib.exe, Dtcsetup.exe, Dtsffile.dll, Dtsffile.rll, Dtspkg.dll, Dtspkg.rll, Dtspump.dll, Dtspump.rll, Dtsrun.exe, Dtsrun.rll, Impprov.dll, Mergetxt.dll, Msdbi.dll, Msgprox.dll, Msvcp71.dll, Msvcr71.dll, Msxmlsql.dll, Msxmlsql.rll, Odbcbcp.dll, Odsole70.dll, Odsole70.rll, Opends60.dll, Osql.exe, Pfclnt80.dll, Pfclnt80.rll, Rdistcom.dll,

	Replagnt.dll, Repldist.dll, Repldp.dll, Repldsui.dll, Repldts.dll, Replerrx.dll, Replmerg.exe, Replprov.dll, Replprox.dll, Replrec.dll, Replres.rll, Replsub.dll, Replsync.dll, Rinitcom.dll, Scm.exe, Semmap.dll, Semmap.dll, Semmap.rll, Semmap.rll, Semnt.dll, Semnt.dll, Semnt.rll, Semnt.rll, Snapshot.exe, Spresolv.dll, Sqdedev.dll, Sqladevn.rll, Sqladhlp.exe, Sqlagent.dll, Sqlagent.exe, Sqlagent.rll, Sqlatxss.dll, Sqlatxss.rll, Sqlboot.dll, Sqlcmdss.dll, Sqlcmdss.rll, Sqlctr80.dll, Sqldata.dll, Sqldistx.dll, Sqldmo.dll, Sqldmo.rll, Sqlevn70.rll, Sqlimage.dll, Sqlinitx.dll, Sqlmaint.exe, Sqlmangr.exe, Sqlmangr.rll, Sqlmergx.dll, Sqlredis.exe, Sqlrepss.dll, Sqlrepss.rll, Sqlresld.dll, Sqlresld.dll, Sqlresld.dll, Sqlservr.exe, Sqlsnmp.dll, Sqlsort.dll, Sqlsrv32.dll, Sqlsrv32.rll, Sqlstbss.exe, Sqlstbss.rll, Sqlsvc.dll, Sqlsvc.dll, Sqlsvc.rll, Sqlsvc.rll, Sqlunirl.dll, Sqlvdi.dll, Ssmsad70.dll, Ssmslpcn.dll, Ssmsrp70.dll, Ssmssh70.dll, Ssmsvi70.dll, Ssnetlib.dll, Ssnmpn70.dll, Ssradd.dll, Ssravg.dll, Ssrdown.dll, Ssrmax.dll, Ssrmin.dll, Ssrpub.dll, Ssrup.dll, Svrnetcn.dll, Svrnetcn.exe, Svrnetcn.rll, Ums.dll, W95scm.dll, Xplog70.dll, Xplog70.rll, Xpqueue.dll, Xprepl.dll, Xpsqlbot.dll, Xpstar.dll, Xpstar.rll
Impact	Remote Code Execution

MS09-005	**Vulnerabilities in Microsoft Office Visio Could Allow Remote Code Execution (957634)**
Description	This security update resolves three privately reported vulnerabilities in Microsoft Office Visio that could allow remote code execution if a user opens a specially crafted Visio file. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.
Payload	Dfdc.dll, Dwgcnvt.dll, Gdiplus.dll, Mso.dll, Umlc.dll, Umlsystem.dll, Visio.exe, Visiodwg.dll, Vislib.dll
Impact	Remote Code Execution