

Good News on application compatibility for clients wishing to deploy Microsoft's service pack 3 for Windows XP

An assessment of the application compatibility impact of the new service pack update from Microsoft

Gregory Lambert
Grant Ford

17-March-2008

Headline results

Changebase AOK has carried out an independent study to assess the impact of Microsoft's newly released Service Pack 3 for XP on application estate's compatibility. In the study AOK checked circa 1000 applications for possible issues with the updates contained within XPSP3. It found that the likely negative impact of deploying this service pack for an organisation was low in terms application compatibility issues. While there are a few changes that could cause an application to fail these are likely to affect a very small percentage of the whole portfolio. In general the changes that are included in SP3 have been in the environment for up to a year and are well tested. The most attention in our opinion should be paid to the hotfixes that are rolled up into this release. However, even these have been deployed with a number of customers for some time now and are unlikely to cause serious issues in the majority of cases where applications are reliant on the components that have changed. AOK is easily able to identify the applications that might suffer serious compatibility problems. It can also highlight those that are exposed to areas that will possibly have an effect on the applications on the portfolio so that targeted testing can take place. This is all good news for customers that are on XP and wish to upgrade to the latest service pack and take advantage of the security and functionality enhancements.

XPSP3 summary

The latest service pack release is a continuation of the Microsoft upgrade journey. Most of these changes are already available and in many cases will have already been installed by organizations as part of the regular windows update service. The difference between XPSP2 and SP3 is minor and does not introduce the sort of update that would cause any further "serious" application compatibility concerns.

- No new major functionality or restrictions
- Mostly covered by Windows update: i.e. Minimal impact for most users
- Continuation of a journey from Windows XP (includes SP1, SP2)
- Includes all of the security restrictions and compatibility concerns associated with XP SP2

In summary, it appears that the configuration and OS level changes included in Microsoft's Windows XP Service Pack 3 will have a limited impact on application stability and compatibility and given the many security updates and application updates included, it appears that XPSP3 should strongly considered for rapid deployment for most organisations.

The detail

The collection of Microsoft updates that comprises the recently released Window XP Service Pack 3 (XPSP3) is a culmination of the following groups or "clusters" of updates including;

- 🕒 A Microsoft Common Control Update (COMCTL)
 - A roll-up of Windows Security updates
 - A Microsoft middleware update (Microsoft XML)
 - A collection of tested and approved Microsoft Hotfixes
 - The revocation of 3 rarely used API calls (relating to DEP)
 - A roll-up of a series of application updates that have been released since XP Service Pack 2

When referring to the potential impact on applications' stability or installation, there are two primary factors to consider when deploying a Service Pack upgrade; the likelihood of the issue occurring and the severity of a particular the particular issue.

After reviewing the compatibility and impact analysis results of just under 1000 application packages from a variety of sources and industries, we have developed the following views on each of the XP Service Pack 3 sub-groups or clusters;

1. Microsoft Common Control Update: This control has been included on the initial release of Windows XP and has a minor update. As this update has been included as part of an OS update, following installation best practices (and using MSI Installer packages) will respect the later versions of this control and so, this update should have minimal impact on application compatibility and stability.
2. The roll-up of several Microsoft Security updates (i.e. MS05-040, MS05-032) have been available for a number of years and all workstations with Microsoft Update enabled should have already received and installed these updates. The impact on application stability will be minimal as any problems should have been discovered many months ago.
3. As with the previous Microsoft control update, there has been an update to the core XML middleware layer. This update has also been available for a number of months and for the most part, most environments will have already deployed this update. This update should have minimal impact on application configuration and stability for most well-maintained and updated system.
4. As issues arise, Microsoft support teams will respond to specific application and operating systems issues with a specified update or "Hotfix". These Hotfix updates progress through the full Microsoft testing regime but may have been exposed to a limited number of customers for deployment. In this instance, these hotfixes will not have had as robust an exposure as other updates and it is possible there could be a limited impact on application compatibility and stability.
5. As part of the Microsoft XP SP3 update, three DEP (memory handling API) calls have been deprecated and formal Microsoft support removed. While this would cause serious issues for an application, the occurrence of applications that would employ these API calls would be rare and so it is expected that this update will have a very limited (very rare) potential for causing application instability.
6. As part of the OS update process, Microsoft has also updated an number of applications such as Outlook Express and the Shadow copy service. These updates have been included in recent Microsoft updates and organisations that have well-maintained and subscribed and deployed recent Microsoft updates should not experience any reduced application stability or compatibility.

To outline the likelihood and potential impact of the updates causing stability or compatibility impact on a given application, the following table outlines the risk for each grouping included in Windows XP SP3.

XP Service Pack 3 Update Clusters	Likelihood Impact	Overall Risk
Application Updates	6	1LOW
Common Control Update	7	1LOW
Core File Update		
DEP API Analysis	1	9LOW
HotFix Analysis	3	5MEDIUM
MMC 3.0 Analysis	1	2LOW

MSXML 3.0 Update Analysis	7	1LOW
Security Roll-up Updates	7	3LOW

The issue of OS upgrades in general

Application compatibility is a serious concern for IT administrators when it comes to migrating their applications to a new operating system or applying a major new service pack. Of primary concern is “when I apply this new service pack to increase my security, will it stop my applications and OS from working?”

Scenarios that would cause serious concern

If we look at the things that will stop an application working they can be broadly broken down into 4 main areas of concern.

- 1 Are there new security restrictions being added that will deny access to the application that it is expecting to find available (this could include being able to write certain files or settings to certain areas)?
- 2 Are there any components being deprecated that this application requires?
- 3 Are there any APIs that this application uses that are being deprecated?
- 4 Has the supported driver model changed in any way such that drivers required by the application will no longer install/function correctly?

In the above cases AOK is able identify the issues of concern and where possible make the necessary configuration changes that will enable the application to install and function correctly. In the cases where the issue cannot be fixed (e.g. it relies on unsupported drivers) it will advise remediation by the vendor.

Scenarios that would cause minor concern

Of lesser concern but something that might still cause an issue in a small number of cases is when a component changes that other applications rely on. In this case the components is usually either

- 1 being enhanced or
- 2 having issues remediated.

However, it is possible that when this functionality is changed that there could be an unexpected/unwanted behavior reflected in the application that is using that service. In these cases where an application is dependent on a component that is changing, AOK will advise testing the application (or the IT department may opt to monitor it for unwanted changes in behavior).

Appendix

AOK XPSP3 Report Plugin Summary

1. Windows XP SP3 Application Updates

This AOK Application WorkBench Plugin analyzes each loaded package for configuration data that is also included in the following updates:

- 900930 - Outlook Express Updates, 903234 - An update is available to optimize Volume Shadow Copy Service
- 885932, 886677, 888240, MS05-020 - IE 6 updates,
- 884883 - Common Control (COMCTL) update
- 819978 - COM+ Application update.

This Plugin analyses both the contents of the application package and its dependencies down to the core OS file level.

For further information please refer to the ChangeBASE website. The recommended remedy for this type of issue is a full UAT testing process prior to deployment .

2. Windows XP SP3 Common Control Update

This AOK Plugin analyses each loaded and selected application for configuration data (files and registry settings) that are included in the common controls that have been updated since Windows XP Service Pack 2. This Plugin analyses both the contents of the application package and its dependencies down to the core OS file level. For further information please refer to the ChangeBASE website. This Plugin analyses both the contents of the application package and its dependencies down to the core OS file level. The recommended remedy for this type of issue is the removal of the offending files and related configuration data and the completion of a full UAT testing process prior to deployment .

3. Windows XP SP3 DEP API Analysis

This report analyses each loaded application for dependencies on the updated Data Execution Protection (DEP) functionality. These new API's affect the Windows XP security model and include SetProcessDEPPolicy, GetSystemDEPPolicy and getProcessDEPPolicy. For further information, please reference the Windows XP SP3 overview documentation. The recommended remedy for this type of issue is a full UAT testing process prior to deployment.

4. Windows XP SP3 HotFix Analysis

This AOK Plugin analyses each selected and loaded application package for files and configuration data which may be present or analyses this package as dependency on the files and configuration included in the large number of hotfixes and QFE updates released prior to Windows XP Service Pack 3. This Plugin analyses both the contents of the application package and its dependencies down to the core OS file level. For further information on the detailed list of what hotfixes are included, please refer to the ChangeBASE website. The recommended remedy for this type of issue is a full UAT testing process prior to deployment.

5. Windows XP SP3 MMC 3.0 Analysis

This AOK WorkBench Plugin analyses each loaded and selected application for files and configuration data that overlaps at package level and as a

dependency any files or configuration data contained with the Microsoft MMC 3.0 update (KB907265). This Plugin analyses both the contents of the application package and its dependencies down to the core OS file level. The recommended remedy for this type of issue is the removal of the offending files and related configuration data and the completion of a full UAT testing process prior to deployment.

6. **Windows XP SP3 MSXML 6.0 Component Analysis**

This AOK Plugin analyzes each loaded and selected application to ensure that there is not "conflict" or overlap between the selected application packages file and configuration data and the components contained within the Microsoft MSXML 6 update. This Plugin analyses both the contents of the application package and its dependencies down to the core OS file level. The recommended remedy for this type of issue is the removal of the offending files and related configuration data and the completion of a full UAT testing process prior to deployment.

7. **Windows XP SP3 Core File Update Analysis**

This AOK Plugin analyzes each loaded and selected application to ensure that there is not "conflict" or overlap between the selected application packages file and configuration data and the components contained within the release of Windows XP Service Pack 3. This Plugin analyses both the contents of the application package and its dependencies down to the core OS file level. The recommended remedy for this type of issue is the removal of the offending files and related configuration data and the completion of a full UAT testing process prior to deployment.

8. **Windows XP SP3 Security Update Cluster**

This AOK Plugin analyses loaded applications for conflicts and overlaps with the following Microsoft Updates which are included in the Windows XP Service Pack 3:

- MS05-039; Vulnerability in Plug and Play could allow remote code execution and elevation of privilege.
- MS05-041; Vulnerability in Remote Desktop Protocol could allow denial of service.
- MS05-042; Vulnerabilities in Kerberos could allow denial of service.
- MS05-038; Cumulative security update for Internet Explorer.
- MS05-040; Vulnerability in Telephony service could allow remote code execution.
- MS05-043; Vulnerability in Print Spooler service could allow remote code.
- MS05-018; Vulnerabilities in Windows kernel could allow elevation of privilege and denial of service.
- MS05-008; Vulnerability in Windows shell could allow remote code execution.
- MS05-016; Vulnerability in Windows Shell that could allow remote code execution.
- MS05-001; Vulnerability in HTML Help could allow code execution.
- MS05-032; Vulnerability in Microsoft agent.

The recommended remedy for this type of issue is the removal of the offending files and related configuration data and the completion of a full UAT testing process prior to deployment.