



DIY Service Pack

Article: <http://www.heise-security.co.uk/articles/80682>

Download: <http://www.heise.de/ct/projekte/offlineupdate/>

Installing Windows updates without an internet connection

Looking for manageable Windows updates even without an internet connection? Our offline update 3.0 script collection downloads the entire body of updates for Windows 2000, XP or Server 2003 from Microsoft's servers in one fell swoop and then uses them to create patch packages on CD, DVD or USB stick. Those in turn allow you to update as many PCs as desired.

Have you installed Windows XP fresh from the original CD and then headed over to the update website lately? If not, be ready for an unpleasant surprise. For a system running XP Service Pack 2, the website recommends that you download 60 updates at an overall data volume of around 40 MBytes. And don't forget: that number keeps growing with each Patch Tuesday, as the monthly event of new patches released each second Tuesday of the month has been dubbed.

For its part, the Redmond crew doesn't see the update flood as any reason to rush the release of a third Service Pack for XP - all indications are that any potential SP3 would come out in the second half of 2007 at the very earliest [1]. For better or for worse, until that next service pack does roll off the assembly line, users will have to connect their PCs to the internet to bring their OS up to date.

The update dilemma

Anyone installing Windows fresh from a CD or who acquires a PC with a preinstalled instance of Windows is in a tricky situation: to protect the machine against the various dangers of the internet, one must first install all current security updates to plug the countless holes in Windows and Internet Explorer. To fetch a copy of the updates, however, Microsoft requires that your computer be connected to the internet.

That is risky: anyone using a slow modem to surf the net will have to wait several hours until the 60 updates - some 40 MB in all - dribble their way through the connection. In the meantime, one visit to a rigged website is enough to let a bug get a crucial first foothold in the machine.

The situation is particularly precarious for Windows 2000 and Windows XP without Service Pack 1, as these versions have no built-in firewall and hence are helpless against the omnipresent worms circulating on the internet. A virgin system of this kind brought online can be compromised before you can even install a security update.

Microsoft offers its users no practical solution for installing the new updates onto a PC via removable storage media. It is true that the security bulletins on Microsoft's web pages do also provide all updates as packages that can be individually installed - even in ISO image form containing all updates released on a given Patch Tuesday (see KnowledgeBase article 918096).

But what Microsoft doesn't provide are convenient installation scripts. This means that manual installation sometimes fails simply because of sheer number of updates involved. It's almost impossible to establish a list of patches required for a naked copy of Windows without the aid of the Windows Update mechanism.

An alternative

We here offer an alternative to this update dilemma, starting immediately: version 3 of our script collection Offline Update requires only a few steps to reel in a current service pack at any time, combining all released Windows updates at the time of download. The download script acquires the complete update library for selected operating systems from Microsoft's servers and uses them to create ISO images for CDs or DVDs as desired. These in turn can be used to update as many PCs as you wish.

Torsten Wittrock of the IT Centre at the University of Kiel rebuilt the script for version 3.0 from the bottom up. With the previous version, each new Patch Tuesday meant that the latest updates had to be manually integrated into the scripts. Version 3.0 automatically incorporates the newly released patches and supports Windows 2000, XP and (for the first time) Server 2003 - including the English versions. The current version of the solution only covers security updates that affect Windows itself. In contrast, the online mechanisms also bring other Microsoft products up to date, including Office and the IIS Webserver.

The following demonstrates how to put together a current service pack using the scripts, how to install it on a target PC and what further options are available to you.

Compiling a service pack

Unpack the zip archive onto a hard drive with sufficient space for all the Microsoft updates that will be downloaded, and that can also accommodate the ISO images created from them. Downloading updates for all three supported English operating systems and creating a DVD image from it can amount to almost 3 gigabytes.

The download script is best used on a PC with a fast internet connection and complete with all patches. It draws several hundred megabytes off the net during the first working pass, although it will not then need to reacquire that data once the package is updated after a later Patch Tuesday.

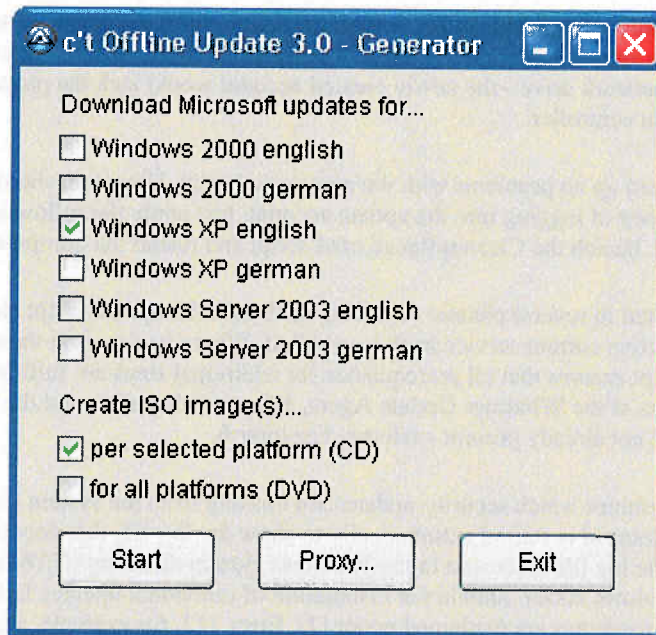
When unpacking the archive, mind that its directory structure is preserved. Subdirectories into which the script sorts the update packets and ISO images are predefined within the scripts.

Once unpacked, no other preparation is required before using the download script under Windows XP. It retrieves not only the updates from the internet, but also a few additional tools required by the installation script on the target system. These originate from Microsoft, which is why for licensing reasons we cannot deliver them ourselves.

If you wish to use the download script on Windows 2000 or Server 2003, then you still need to copy a working version of the command line tool reg.exe into the client\bin subdirectory. You can find reg.exe on the Windows 2000 installation CD under \support\tools in the support.cab archive. The version of reg.exe included in Server 2003 is not suitable for the update package, since it does not function with other operating systems. You can extract the suitable reg.exe from the Windows\system32 directory of an existing copy of XP.

The download script downloads the complete Microsoft update catalogue, which contains significantly more update packets than are needed to patch a freshly installed system – but only the necessary ones are then installed. For Windows 2000, it draws around 400 MBytes per selected language from the internet; for Windows XP, 600 MBytes each; and for Windows Server 2003, around 700 MBytes. Included in that calculation are 100 MBytes per OS that are identical for all systems -- and which the script does not download repeatedly even if multiple versions are selected. The largest chunks are the respective current Service Packs.

And off you go: double click on DownloadStarterGUI.exe to call up a dialogue box within which you can set which versions of Windows need updates. Restricted user rights are not a problem as long as you have not selected Windows 2000. For the latter, the download script also downloads Internet Explorer 6, which can only be installed with administrator rights - since it remotely controls the GUI of the network installer.



The download script retrieves Microsoft's complete update archive for the selected operating system and uses it to create ISO files for removable installation media.

You can prepare a separate ISO image to be placed on CD for each language of each selected operating system. The script can also build a large ISO for DVD use that can update all selected operating systems. If you do not set any checks in the second area, the script skips the image creation procedure. The finished update packet can also be copied onto a USB stick, for example, or prepared for sharing over a local network.

Click on the start button and then sit back and relax. A window opens and you can watch the tools speedily fulfill their tasks. Fully automated, they download additional programs off the net, determine the download URLs, download the selected updates and then finish up by preparing the ISO images.

Once completed without errors, the ready-to-use update packet containing all patches and their installation scripts can be found in the client subdirectory. The ISO images created from them are in the iso folder. These can then be put onto a blank disc using the burning program of your choice; one free tool for this is [Deep Burner](#), for example. Be sure explicitly to select the function for burning from image files - otherwise you could end up simply creating an archive copy of the ISO file on a data CD.

To use other storage media as installation media, simply copy over the contents of the client folder. The individual updates are located there in the wxp (Windows XP), w2k (Windows 2000) and w2k3 (Windows Server 2003) subfolders. Simply omit any specific operating systems that the target medium doesn't need to cover.

Installation

Double-click on UpdateStarterGUI.exe to launch the installation of the updates on the target PC, or simply insert a CD or DVD with one of the ISO images recorded on it (it will start from the autoplay function). The installation of the missing components and updates may require several reboots. The "Automatic reboot and recall" option allows the script to shut down the PC on its own where necessary and then resume work following the reboot - this is as easy as it gets.

To do this, it creates a temporary administrator account called "WSUSAdmin", to which it then assigns a random password. The script enters that access data into the registry so that Windows automatically logs in as the temporary administrator following the reboot and calls up the update script fresh. After the completion of the final phase, the script deletes the temporary administrator account again. Caution: if the computer is unattended while the update is running in automated mode, it is possible for someone with access to the PC to create administrator rights for themselves without being noticed.

If you do not activate the "Automatic reboot and recall" option, the script will request you to reboot the PC manually from time to time. You must then also restart the program to allow it to finish its work. Automatic log-in is not activated if you call up the installation script from a network drive - the newly created account would lack the proper connection. The function also cannot be used with a domain controller.

Our testing of this procedure turned up no problems with the automatic log-in. However, should something go wrong, and Windows ends up in an infinite loop of logging into the update account, just apply the following emergency brake: interrupt the installation script with Ctrl-C, launch the CleanupRecall.cmd script and restart the computer.

The update installation is conducted in several phases: following each call, the update script checks which operating system is running and whether the respective current service pack is installed. Where necessary it then installs one and requests a restart. In the next phase, the script ensures that all prerequisites for additional steps are fulfilled. Among the components that it then installs are current versions of the Windows Update Agent, Microsoft Installer, and the Windows Script Host. For Windows 2000 it also installs - if not already present - Internet Explorer 6.

In the final phase, the script determines which security updates are missing from the system and installs them one after another. After the final reboot, Notepad is started automatically to show the log-file that documents which patches were applied by the script. The cupdate.log file is located in the Windows system directory (C:\Windows for Windows XP and Server 2003, C:\WINNT for Windows 2000). Should the installation of individual updates fail, then the returned error codes are included there as well. Their meanings are explained under [2]. Error 112, for example, signals that the hard drive is full.



For Windows 2000 only: at this point you should manually start the installation script one last time as a final check - the Windows Update Engine is for some unfortunate reason unable to recognize any missing updates here the first time through.

If all holes have been plugged, then you can link your PC to the internet with peace of mind. Be sure that the system service for automated updates is activated to allow Windows to install future new security updates on its own.

Last details

Our offline update installs only Windows updates classified by Microsoft as being security-related. An accompanying analysis using Microsoft's Baseline Security Analyzer ([MBSA](#)) should confirm that no important patches are missing. In Windows 2000, the script could potentially have missed an update for Microsoft's outdated Java VM (KB816096) that has not been serviced for some time now. Despite all of our attempts, this update cannot be cleanly installed via script. Anyone interested in secure Java applets is advised to switch to the current Java 5 from Sun. For similar reasons, when working with Windows 2000 the script skips over update 832483 for Microsoft Data Access Components (MDAC).

The Malicious Software Removal Tool is omitted by the script. Strictly speaking, it is not so much a security update as a bug fighter that recognizes only a low number of current samples. A real virus scanner with fresh signatures produces significantly better results.

If, having finished the offline update, you then visit the Windows Update website, it will suggest the aforementioned patches as well as a handful of other updates for installation. At the time this article was written, that amounted to eight items for

Windows XP. These packets do not close holes that could be exploited by attackers, but rather resolve smaller Windows problems or are add-in optional components like the controversial WGA notification.

The offline update draws its information from the same Microsoft catalogue file as used by MBSA, which is why both produce the same positive result. Interestingly, those packets missing from the online update are not listed in MSBA's XML catalogue at all. Anyone looking to install those updates offline can enter them in as a static packet (see below for more details).

How it works

When applying the updates, the script uses the same Windows Update Agent that is used with the normal online update. Microsoft upgraded this agent in mid-2005 to conform with the WSUS update server and also arranged for it to have a COM interface through which it can receive script errors. [3]

The update agent draws its information from the wsusscan.cab archive whose current version is made available for download by Microsoft at a static URL [4]. The Microsoft Baseline Security Analyzer (MBSA) also loads that file to determine whether or not the system is completely patched.

The archive contains a catalogue file called package.xml in which Microsoft indexes all security updates (and their dependencies) for all operating systems. The download URLs for all updates are also found there, allowing for direct downloading of the individual items from the Microsoft servers.

The download script that creates the installation media does not inspect the patch status of the PC that has executed it. It uses XSLT (XML Stylesheet Language for Transformations) to fish out the relevant URLs for a specific operating system. It provides Microsoft's XSLT processor with predefined style sheets located in the xslt folder of our script collection. This produces URL lists that are passed to wget, a program that then downloads all of the files. While Microsoft's XML catalogue indexes significantly more updates than are required to bring a freshly installed instance of Windows up to date, our solution accounts for the additional space requirements on the installation media.

Some packets that the installation script is supposed to install, including the current service packs, are not listed in the XML catalogue at all. The download script therefore processes additional text files in the static directory that contain additional URLs. If everything is properly aligned, the script instructs mkisofs to pack the content of the client subfolder into the ISO images.

For later installation onto the target PC, the VB script ListMissingUpdateIds.vbs requests the list of missing packets from the update agents. It draws the catalogue files required for this from the installation media that was created ahead of time. The installation script then installs those updates listed by the agent as missing - another benefit compared with the older version of the offline update, which couldn't check what was already on hand.

Unfortunately, not all update packets obey the same command line switches; this problem is resolved with the compiled AutoIt script RetryingUpdateInstaller.exe: it first attempts to install the packets with the parameters /q /z (no return report, no reboot), which works for almost all of the current packets. If that fails, the script then makes a new attempt with the /Q parameter, which works with older update packets.

Command line

The two programs, DownloadStarterGUI and UpdateStarterGUI, are implemented in the AutoIt scripting language (see www.autoitscript.com). They serve solely as a user interface for the batch scripts DownloadUpdatesAndCreateISOImage.cmd and DoUpdate.cmd, located in the subfolders cmd and client\cmd.

The Windows Task Scheduler allows for regularly scheduled execution of the download batch script, thereby assuring a perpetually fresh on-hand version of the update packet and ISO files created by the script. If you set the download to run every night, you will also be among the first to receive updates released by Microsoft outside of the standard Patch Tuesday schedule.

The download script understands the following command line switches for use with the Task Scheduler:

```
DownloadUpdatesAndCreateISOImage.cmd {w2k | w2k3 | wxp} {deu | enu} [/scheduled]  
[/skipiso] [/proxy http://server:port]
```

The parameters "wxp enu" instruct the script to download only updates for an English version of Windows XP, for example. /skipiso skips the creation of the image files.

If you set up the Task Scheduler also to retrieve current updates for Windows 2000, you must have administrator rights the first time you call up the download script, since the network installer for Internet Explorer 6 cannot work remotely if the Task Scheduler calls up the script. Include the /scheduled parameter in the configuration so that the script does not make a fresh attempt to download the browser.

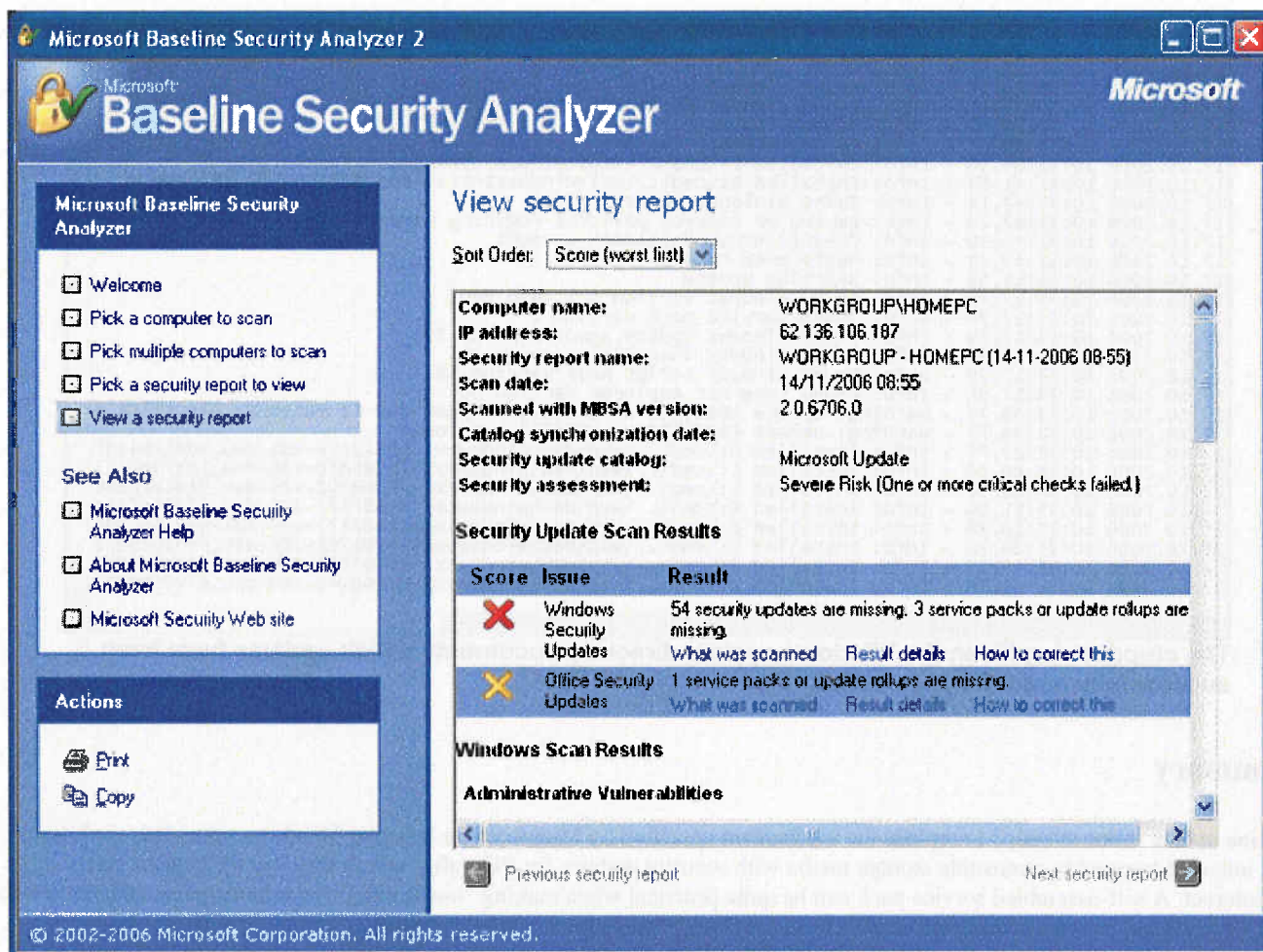
The installation of the update can also be initiated on the target PC using the command line:

```
DoUpdate.cmd [/all] [/autoreboot] [/showlog]
```

The /autoreboot parameter activates the automated reboot function; /showlog opens the log file in Notepad following the conclusion of installation. The [/all] switch, not available in the GUI, forces new installation of all updates, even if they are already installed on the target PC.

Tweaking the parameters

It is possible to prevent the installation of individual updates, such as when it becomes known that a specific patch causes problems. To do so, enter its KnowledgeBase ID into the "exclude-list.txt" file in the \client\exclude folder on the basis of the pattern 123456. The installation script will skip over any updates indicated there, recording that it has done so in the log file.



If run before any updates, Microsoft's Baseline Security Analyzer will show as here that no updates have been installed. Run again after the updates, it will confirm that they are in place.

Additional Microsoft patches not covered in the base configuration of the offline update can be added in later as static updates. To arrange for the download script to download an additional packet, add its URL into one of the text files in the "static" directory. For the English version of XP, for example, this is the file StaticDownloadLinks-wxp-enu.txt. The download script sorts the downloaded files into the proper folder within \client.

To arrange for the installation script to install the additional update, you must add its KnowledgeBase ID into a file within \client\static associated with the applicable operating system; for XP this is StaticUpdateIds-wxp.txt. Because the installation script cannot check whether a static update has already been installed, it basically installs the entire list, even if individual updates are already present.


```

17.10.2006 10:30:37,22 - Info: Starting update
17.10.2006 10:30:38,95 - Info: Found windows version 5.1 (wpx deu)
17.10.2006 10:30:38,97 - Info: Found service pack version 2
17.10.2006 10:30:38,97 - Info: Found windows update agent version 54
17.10.2006 10:30:38,97 - Info: Found windows installer version 30
17.10.2006 10:30:38,97 - Info: Found windows script host version 56
17.10.2006 10:30:38,97 - Info: Found internet explorer version 60
17.10.2006 10:31:04,56 - Info: Installed E:\cmd\..\wsus\windowsupdateAgent20-x86.exe
17.10.2006 10:31:41,84 - Info: Installed E:\cmd\..\msi\windowsinstaller-KB893803-v2-x86.exe
17.10.2006 10:31:42,14 - Info: Saved winlogon registry hive
17.10.2006 10:31:42,26 - Info: Saving of Desktop policies registry hive failed
17.10.2006 10:31:49,30 - Info: Created WSUSUpdateAdmin account
17.10.2006 10:31:49,44 - Info: Registered recall
17.10.2006 10:33:11,53 - Info: Starting update
17.10.2006 10:33:17,78 - Info: Found windows version 5.1 (wpx deu)
17.10.2006 10:33:17,79 - Info: Found service pack version 2
17.10.2006 10:33:17,79 - Info: Found windows update agent version 58
17.10.2006 10:33:17,79 - Info: Found windows installer version 31
17.10.2006 10:33:17,79 - Info: Found windows script host version 56
17.10.2006 10:33:17,81 - Info: Found internet explorer version 60
17.10.2006 10:33:58,75 - warning: update KB816093 or q816093 skipped due to matching blacklist e
17.10.2006 10:33:58,75 - warning: update KB890830 or q890830 not found
17.10.2006 10:34:23,75 - Info: Installed E:\cmd\..\wpx\deu\windowsxp-kb873339-x86-deu_9d612b44df
17.10.2006 10:34:40,09 - Info: Installed E:\cmd\..\wpx\deu\windowsxp-kb885836-x86-deu_10af9ef4c7
17.10.2006 10:34:54,98 - Info: Installed E:\cmd\..\wpx\deu\windowsxp-kb888302-x86-deu_d1d1d2bee8
17.10.2006 10:35:11,00 - Info: Installed E:\cmd\..\wpx\deu\windowsxp-kb887472-x86-deu_8fd36dfa5e
17.10.2006 10:35:16,78 - Info: Installed E:\cmd\..\wpx\deu\windowsxp-kb887472-x86-spi-deu_abc7d4
17.10.2006 10:35:29,20 - Info: Installed E:\cmd\..\wpx\deu\windowsxp-kb891781-x86-deu_f9510c8e23
17.10.2006 10:35:47,10 - Info: Installed E:\cmd\..\wpx\deu\windowsxp-kb885835-x86-deu_c50ab899dc
17.10.2006 10:36:00,98 - Info: Installed E:\cmd\..\wpx\deu\windowsxp-kb890046-x86-deu_e7e25bf0b9

```

The ctupdate.log file in the Windows system directory documents which updates have been successfully applied by the script.

Summary

Offline update is not intended to replace the mechanism specified by Microsoft for bringing Windows up to date via Internet. It is intended to provide removable storage media with security updates for PCs, after which they can be brought safely onto the internet. A self-assembled service pack can be quite practical when making "house calls" for acquaintances or clients who lack a broadband internet connection or who have previously been skittish about patching.

The update packet created through the scripts can also be shared over a local network – with the caveat that in the current version the automatic reboot function cannot be used for network installations. Through its WSUS update server, Microsoft offers a more powerful solution for keeping PCs in a larger LAN up to date. The server is used to set in detail just which updates are to be installed on which PC groups. WSUS also reports back which have already been provided.

Our update scripts are superior in several ways to similar solutions circulating on the internet. For starters, "update packs" prepared by third parties (and which Microsoft has in no way authorized) are a dubious source of security updates. Our script by contrast draws updates directly from Microsoft's internet servers, independently of whether the PC running the download script has been fully patched or not.

The offline update is set up modularly and is easy to adjust. It would also be conceivable to use the mechanisms employed there to install updates for other Microsoft products such as Office. The version available at press time, 3.0, passed our tests – although it cannot be ruled out that one bug or another may turn up over time. We have set up a [forum](#) and invite you to discuss your experiences or problems there and suggest further enhancements.