GFI White Paper

Patch management: Fixing vulnerabilities before they are exploited

Managing and administering software updates remains one of the most challenging and resource-intensive tasks an IT Department undertakes on a daily basis. This white paper examines the important role played by patch management to help organizations keep their PC real estate fully up-to-date with the latest security patches, without unduly compromising reliablity, productivity, security and data integrity.

GFI®

Contents

Introduction

Managing and administering software updates remains one of the most challenging and resource-intensive tasks an IT Department undertakes on a daily basis.

While software updates serve many important roles, be it delivering feature improvements or fixing bugs and security vulnerabilities, they bring with them a number of potential challenges for the IT Department in terms of ensuring systems are up-to-date, that new problems are not introduced by patches designed to fix things, and updates do not create compatibility or instability issues. All this needs to be done while ensuring that updates are pushed to PCs as quickly as possible to prevent vulnerabilities being exploited. The constantly evolving software landscape makes patch management an important consideration for all IT decision makers, regardless of organization size.

Software that is not kept up-to-date with the latest patches and version updates runs the risk of creating weak points in your organization's security strategy, placing servers and client devices at risk from exploitation by malware, hacking attacks, as well as increasing the risk of reliability-based failure and data loss. The number of vulnerabilities in software commonly found on client PCs grew by 71 percent between 2009 and 2010 . This jump is due in large part to problems occurring within third-party applications, rather than with issues directly related to the underlying Windows operating system (OS) or Microsoft-produced application software.

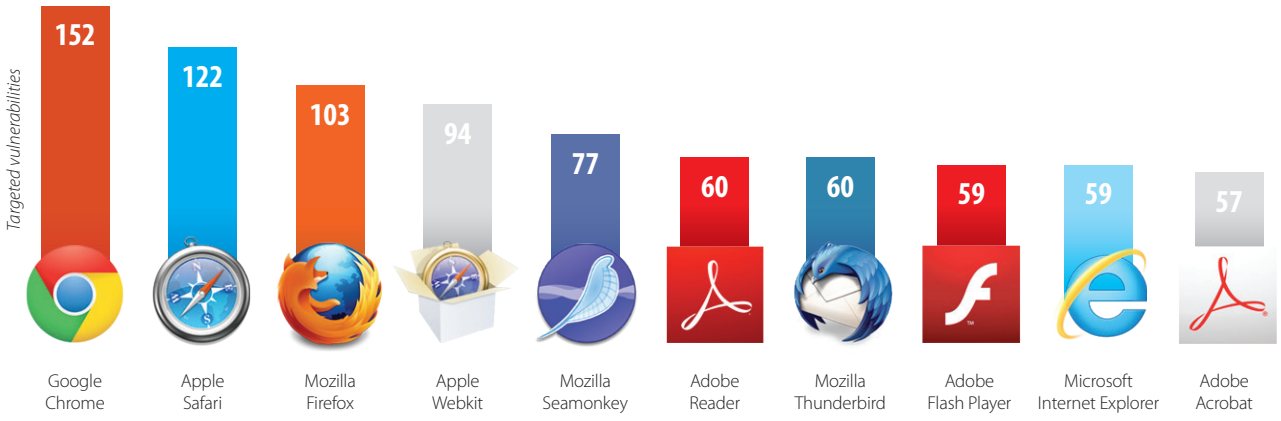
Effective patch management improves reliability and IT efficiency, automating many of the administrative tasks associated with deploying software updates while minimizing the amount of downtime associated with patch deployment, patch auditing and patch roll-back.

Importance of patch management

The process of keeping a PC or a server fully patched is easier today than ever, thanks in part to the moves of several key software vendors to build automated update checking into their applications, as well as the highly-developed Microsoft update service, which can download and, in many cases, install updates in the background without requiring user input or a system reboot. Nonetheless, the installation of patches, if left solely to the user, can be overlooked, leading to known vulnerabilities being left unaddressed and ripe for exploitation.

By virtue of being an application and OS vendor, Microsoft attracts the most attention when it comes to issuing and installing software updates. However, the majority of known application vulnerabilities continue to come from third parties, while the smallest percentage of threats resides in the OS itself. The implications of third-party software on PC security and reliability is further challenged by the role of browser plug-ins, media player codecs and other bolt-on code that works in conjunction with an existing application or system service.

The vulnerability challenges posed by third-party applications can best be illustrated by looking at the most targeted applications. Using 2010 data from the US National Vulnerability Database, we can see that of the top 10 applications targeted for vulnerabilities, ranked by total number of targeted vulnerabilities, nine were third-party applications:



Microsoft Internet Explorer, the highest ranked Microsoft application, was also the highest ranked OS-installed application on the list sharing sixth place with Adobe Reader. Microsoft Office, the company's highest-placed add-on software product, placed 11th. Oracle's Java Runtime Environment, often targeted when vulnerabilities are revealed by the release of a patch, placed 12th.

The data also illustrates how web browsers continue to be the weakest point when it comes to software-based vulnerabilities.

In terms of operating systems, various versions of Microsoft Windows dominate the field by virtue of the sheer market penetration of the OS, while Linux and both the server and desktop versions of Mac OS X follow very close behind. In fact, in 2010 the desktop versions of Mac OS X experienced 96 targeted vulnerabilities compared to 88 for Windows Vista and 66 for Windows 7, the latest incarnation of the OS.

Managing software updates and critical patch deployment manually will quickly increase the maintenance overhead associated with applications and the operating systems they run on, to the point of overwhelming the IT team. For example, the volume of software updates and critical vulnerability patches issued by the average vendor varies, but in the case of market leader Microsoft, the size of its monthly 'Patch Tuesday' software update payload can be significant.

In April 2011 alone, Microsoft delivered 64 critical fixes across 17 software updates, while the previous month it fixed just four known flaws with three updates. In February 2011, Adobe patched 42 known bugs and vulnerabilities in its Adobe Reader and Flash products, while Oracle patched 73 known security vulnerabilities across its entire product line in April 2011. The latter is an example of how complex patch management can be if not automated, as Oracle's patching applied to both organically-developed products as well as a number of high-profile acquired products that still sit outside the core Oracle code set such as JD Edwards, PeopleSoft, Siebel and OpenOffice.

These are just a few examples of a much larger software patching landscape that affects all software vendors. These are also examples of how little predictability there is in the volume and severity of the patches being issued; and with it the resources that will be needed to ensure they are installed.

Balancing security with reliability

Various steps have been taken by operating system and application vendors to simplify the process and to minimize the window during which a machine is exposed to a known application or underlying OS vulnerability, such as integrating automated update download mechanisms and pop-up windows to alert users on the availability of a new update, as well as offering educational notes on why the user needs to deploy the update.

Such services have a weakness in that they rely on users who actively connect to the Internet and allow updates to be downloaded and installed. The ease with which end-users can update their own machines, coupled with the benefits of encouraging them to do so, also means that the IT department needs to maintain visibility of what patches have been installed in the event that a problem arises.

Even a fully-patched machine can present problems for both the user and the business. For example, in February 2010 Microsoft issued a patch for Windows XP, called MS10-015. The patch, intended to fix long-standing security vulnerabilities in the OS, was found to create significant system instability in certain configurations of PCs, leading to the unrecoverable 'Blue Screen of Death' Windows error.

The error led to the temporary suspension of the patch from Microsoft's Windows Update patch download service while the instability issues were investigated and fixed. For users that had already installed the patch, the most prudent cause of action was to uninstall the patch and roll the system back to the previous good state.

The ability to roll back a patch is essential to ensure a swift remediation of software problems caused by the installation of a software update. There are numerous reasons why an organization might need or choose to revoke a software update that has been pushed out by a vendor and installed:

- Instability – As with the example above, the wide range of potential configurations and software combinations on a PC can mean that even a well-tested software patch can cause a machine or application to malfunction after installation.
- Compatibility – Upgrades can create problems including implementing changes to file formats, database structures, storage formats and communication protocols that have not been carried through the IT estate, or which have not been adopted by a customer or supplier, thus breaking workflow.
- Driver clashes – In instances where the software update makes extensive changes to the way the software interfaces with hardware, it may be necessary to uninstall a patch and hold off deploying until hardware drivers have been updated to restore compatibility with the operating system or application.

While other solutions exist for patch management, such as Microsoft's own Windows Server Update Services (WSUS), these solutions are usually limited in both their scope and ability to automate the patch management process. In the case of WSUS, patch management is limited to only Microsoft applications and system patches issued through the Microsoft Update framework. Third party solutions are not catered for, while the ability to revoke and remove a patch that has already been installed is reliant on the operating system, successfully creating a Microsoft Restore Point at the time the patch was added, meaning that rolling back a system can result in other perfectly working third party applications being uninstalled in the process.

Solutions for effective patch management

The integrated mechanisms for delivering patches and other software updates to applications and operating systems form just one part of the process. For any organization, the key is to deploy an all-encompassing patch management solution that can automate the process of managing patch deployment and provide quick and easy visibility of the current state of patching on all machines.

A solution such as GFI LanGuard® delivers complete suite of patch management tools in one application. With it, IT administrators can monitor the IT estate to provide a single view of what has been installed on each connected client or server, and trigger automated detection, downloading and deployment of missing patches to ensure a machine is fully patched before it becomes a problem. This approach ensures that known vulnerabilities are addressed before they are exploited; and therefore drastically reduces the maintenance burden placed on IT personnel.

In addition, the patch management solution should provide administrators with an effective means to roll-back problematic patches, returning the machine to its pre-patch state in the event of compatibility or instability issues arising after the installation of an update. This feature is independent of Microsoft's Restore Point technology and applies to both system and third party patches.

Summary

The process of patch management has, over time, been complicated by the growth in operating system and application patches, along with driver updates, many of which are delivered to servers and clients via vendor-operated automated update services but without the safety net of pre-testing to ensure broad compatibility and stability with a wide range of custom configurations of server or desktop PC.

Patch management plays a critical role in ensuring that companies can keep their PC real estate fully up-to-date with the latest security patches and software updates, without unduly compromising reliability, productivity, security and data integrity.

A robust patch management solution that combines swift roll-back of problem patches with a single view of what patches are installed on machines across the organization, is a critical component of both software management and IT security strategies. As part of a wider IT security policy, such a solution will ensure that applications are not placed at unnecessary risk, while ensuring that a policy of encouraging end-users to accept and install critical updates at the first possible opportunity can be maintained.

About GFI®

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMBs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

GFI 3261 may13

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

33 North Garden Ave, Suite 1200, Clearwater, FL 33755, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit http://www.gfi.com/contactus