

## Patch management with WinReporter<sup>®</sup> and RemoteExec<sup>®</sup>

---

*This white paper provides an overview on how to use WinReporter<sup>®</sup> and RemoteExec<sup>®</sup> in conjunction to keep Windows<sup>™</sup> systems updated and immune to most attacks and malicious mobile code.*

## The missing patch : Windows main vulnerability

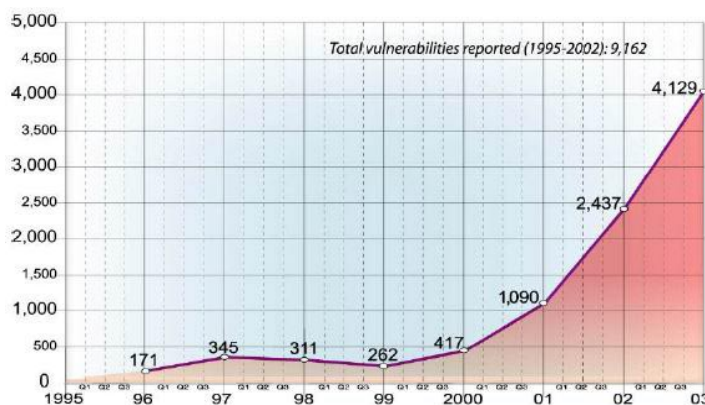
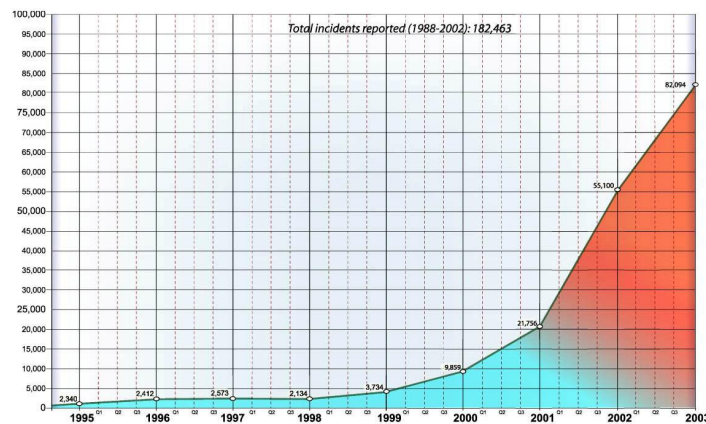
Vulnerability assessment is central to network security. Even though it is good practice to restrictively grant privileges to users, enable relevant auditing events, and disable unnecessary services, these one-time measures are not sufficient.

New vulnerabilities are publicly reported on a daily basis, providing attackers with new means to compromise networks' security. SANS/FBI's top 20 list<sup>(1)</sup> gives the most critical internet security vulnerabilities, and most of them can simply be fixed by applying the suitable update.

As a result, patch management is an ongoing process consisting of scanning machines on the network for missing patches and deploying those patches quickly & efficiently. This has therefore become a key network administration task.

Experience has too often shown that administrators fail to timely apply critical patches: as a consequence, worms (Code Red, SQL/Slammer, etc.) exploit known vulnerabilities, and quickly spread, putting the corporate survivability at risk.

As a matter of fact, the CERT® Coordination Center<sup>(2)</sup> has published vulnerabilities and incidents reported from 1995 to 2003:



Two observations: first, both charts map each other, demonstrating the link between those metrics; secondly, the number of incident-vulnerabilities is very high & spiralling upwards all the time.

This situation is mainly due to the fact that patch management is a time-consuming & daunting task. According to an Aberdeen Group's survey<sup>(3)</sup>, security patch deployment for operating systems cost enterprises in excess of \$2 billion in 2002, and the costs will continue to increase.

(1) <http://www.sans.org/top20/> SANS/FBI: The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus

(2) <http://www.cert.org/>

(3) <http://www.aberdeen.com/2001/research/06030015.asp> Aberdeen Group, security perspective. Surfing the Security Patch Tidal Wave.

## WinReporter® and RemoteExec® patch management philosophy

---

So, there is no question about how crucial patch management is to ensure network security, as a computer is in a far better security state once it has been updated.

However, there is an issue, as some updates can introduce incompatibilities with software used in production, and this can result in severe disruption to the business process.

Therefore, there are 2 distinct approaches that administrators can take:

- ▶ *The “brute-force” automation of patch deployment*  
*Microsoft’s Automated Update* is a good example. It promptly applies all upcoming updates. Microsoft provides a convenient feature to do that - all the end user has to do is enable the automatic update option. Although this alternative is convenient, administrators have to know how far they trust Microsoft updates...
- ▶ *The approach taken by WinReporter® and RemoteExec®*  
This consists of thoroughly testing the latest updates on dummy computers that mirror servers and workstations used in production before any deployment.  
Arguably this is more time consuming, but it is also the safer way to prevent any subsequent problems.  
Information security is a trade off between convenience and assurance; WinReporter® and RemoteExec® have clearly made their choice: assurance.

The core value of this approach is the ability to separate the analysis and the deployment processes, offering meaningful reports on the analysis side with WinReporter®, and hands-free automation on the deployment side with RemoteExec®.

Additionally, these 2 software products offer some features that Windows Automatic Update badly lacks:

WinReporter®:

- ▶ scans selected computers looking for installed (or not) Service Packs, patches, and hotfixes
- ▶ edits meaningful reports to find out which updates are missing
- ▶ edits meaningful reports to build confidence in the network security state

RemoteExec®:

- ▶ deploys patches on Windows versions older than Windows 2000, namely NT 4.0
- ▶ can deploy custom patches for third party software
- ▶ can deploy Windows Installer packages

## WinReporter® & RemoteExec®: the winning team

---

### Scanning for updates with WinReporter®

WinReporter® is a powerful scanning and reporting administrative tool. It remotely inventories software and device configuration as well as user settings, and provides administrators with 50 “out-of-the-box” reports to better manage ongoing corporate-wide patching activities.

Additionally, administrators can create reports for management to demonstrate what systems have been patched, where missing patches may exist, and whether systems are in compliance with corporate standards.

In the patch management context, WinReporter® can both spot computers with missing updates, and provide an accurate picture of the updating state of computers.

To detect vulnerable computers, WinReporter® provides the following functionality:

#### **Reports > Windows NT > Services Packs & hotfixes**

Once there, administrators can easily spot outdated computers. WinReporter® will detect all computers that match the query based on OS version, Service Pack, IE Version, IE Service Pack, and finally hotfixes.

The displayed report lists all computers with missing updates; administrators will use this list as an input to update these computers with RemoteExec®.

There are two ways to handle update analysis with WinReporter®:

- ▶ To detect all computers which match a hotfix configuration

#### **Reports > General > Generic Query, then select the hotfix table**

By doing this, the administrator will get a report listing all computers matching the query.

- ▶ To obtain a comprehensive report with the update state of the overall network

#### **Reports > General > Global report**

Go to the computers part of the report, check the very beginning of each computer part to find out the Service Pack level, and hotfix subpart to find out which hotfixes have been applied.

In the configuration management scheme, it is important to be able to determine the computer configuration state at a given point in time, and this statement applies to the updating configuration.

If anything goes wrong, this information might be useful in discovering a missing update that could have been the reason for the disaster, and can be used to restore the system to its previous state.

## Remote updating with RemoteExec®

RemoteExec® is a powerful generic remote administrative tool.

Its functionalities range from remote reboot to remote program execution. Just bear in mind that RemoteExec® can do much more than patch application.

Although RemoteExec® solely relies on administrators' decision to deploy updates, the deployment is swift and straightforward.

The first step is to retrieve the appropriate update from the developer's Web site. Then, install and perform a thorough set of tests in order to gain assurance that the tested update will not harm in any way the patched system. It is imperative to test all patches before rolling.

Once tested, it can be sent automatically with a single click.

It is worth noting that there are different kinds of updates, see *Microsoft Guide to Security Patch Management (page 27)* <sup>(4)</sup>, each with their specific deployment process. There are 5 kinds of updates that RemoteExec® can deal with:

- ▶ Service Packs and hotfixes for Operation Systems
- ▶ Service Packs and hotfixes for Internet Explorer
- ▶ Updates for Microsoft Office, \*.msp files
- ▶ Few unusual Microsoft updates
- ▶ Third party software updates

## RemoteExec® added value

What distinguishes RemoteExec® from usual patch management tools is the way it deploys patches. It easily deploys typical Microsoft updates, hotfixes, Services Packs, and so forth. Additionally, it can deploy all kind of executables, including the most weird third party software updates.

In the rare cases where user input is needed, administrators can sent out a net send pop up to every user at once through the RemoteExec® file execution tab. This is a definitive advantage on some patch management software that can just handle regular Microsoft updates.

For higher assurance, RemoteExec® clearly distinguishes between Operating System and Internet Explorer updates. Internet Explorer has been involved in numerous security-related vulnerabilities since 2000. Special attention should be directed to ensuring that Internet Explorer is properly patched. Internet Explorer inventory is necessary because there are so many different versions in use, each with its own vulnerabilities. Hence, in the RemoteExec® GUI, Service Packs and hotfixes have specific fields for both Operating System and Internet Explorer.

Other remarkable features of RemoteExec®:

- ▶ RemoteExec does not need an Operating System with a minimum update level to work properly.
- ▶ RemoteExec does not need any third party software to operate unlike a number of competitors that need Microsoft IIS to deploy updates, or a dedicated server to work.
- ▶ RemoteExec® patch deployment saves Internet bandwidth. It downloads all updates for clients to a local mirror, thus limiting external communication to the Internet and reducing the load of valuable external access while facilitates the enforcement of network restrictions.
- ▶ RemoteExec® allows administrators to quickly fix an announced vulnerability. Say a new worm is rapidly spreading across the Internet, and that a given update has to be applied to protect systems - the question is, which machines on the system need the update.  
RemoteExec®, allows you to detect all computers with the missing update in just one click, the next click will deploy the update on those machines.

*NB : Some utilities like Microsoft Baseline Security Analyzer (MBSA), take the process at reverse, first choose the computer, then list all applied updates. To quickly fix a specific hole, this is not a very convenient approach.*

(4) <http://microsoft.com/downloads/details.aspx?FamilyId=73AC38B7-5826-421D-99E8-CDCC608B8992&displaylang=en>  
 The Microsoft Guide to Security Patch Management

## WinReporter® added value

WinReporter® empowers diligent patch management. Accurate and current knowledge of what is present in the environment is essential for maintaining a smooth-running patch management process. WinReporter® hardware and software inventory retrieves specific information by default, such as computer drive information, video card attributes, and RAM amounts, as well as details of installed software and patches and other information that is required to support the end-to-end patch management process.

According to Microsoft<sup>(5)</sup>, the reporting capabilities of Windows Update (WU) or System Update Server (SUS) range from “poor” to “fair”. The amount of information gathered by WinReporter® is massive and easy to manage.

WinReporter® can also make the disaster recovery process easier. Keeping the latest configuration of computers is a wealthy source of information to rebuild a similar computer in order to quickly resume the normal business process.

## Deploying updates with RemoteExec®

Let us discuss how to deploy with RemoteExec® each of the earlier mentioned updates in turn.

### Service Packs and hotfixes

Service Pack and hotfixes deployment process for both Operation System and Internet Explorer is much the same:

- ▶ Right click *action Type* then check *Hotfix/Update or Service Pack installation*.
- ▶ Browse and select the update file.
- ▶ Most releases automatically fill the configuration fields of both *action* and *Filter* tabs; alternatively you can choose your own settings.
- ▶ Go to *computers* tab, select the computer set to be updated.
- ▶ Execute the deployment.

### Microsoft Office update from server location

The Microsoft Office update deployment is somehow different assuming that Microsoft Office is installed from server location.

- ▶ Administrator has to update the server location file running the `msiexec` command.
- ▶ Then synchronize with RemoteExec® (Update operation off the `msi` installation action) all networks' computers with the server location file in order to complete the update process.

A fully explained example is provided by Microsoft<sup>(5)</sup> (see Administrative Update section).

### Unusual Microsoft updates

Microsoft sometimes releases updates that do not observe the standardized structure of hotfixes or Service Packs. Nevertheless, those updates can be applied in exactly the same fashion to regular updates.

### Third party software updates

The deployment process for third party software updates is slightly different.

- ▶ Right click *Action Type* then check *File Execution*.
- ▶ Browse and select the update file.
- ▶ Administrator should contact the third party software editor in order to know which parameters to type for a seamless remote execution.

(5) <http://support.microsoft.com/default.aspx?scid=kb:en-us:Q325671> The Microsoft XP Office updates deployment from server location (page 55)

## Conclusion

---

New breaches that endanger corporate networks are discovered daily.

They might be introduced by the Operating System itself, by a software closely binding to the Operating System, or by third party software.

Networks remain not updated mainly due to the fact that it is a cumbersome task.

WinReporter® quickly spots the computers needing an update, while RemoteExec® boosts the deployment process whatever the update.

Finally, WinReporter® can create useful reports to determine the updating state of the network at a given point in time.