Secunia
Stay Secure

There is no canned approach to patching

There is no canned approach to patching

When attempting to infiltrate and exploit enterprises, cybercriminals will target ALL programs and continually switch their focus to programs with the highest exploitation success rate. Consequently, the threat levels of programs are fluctuating up and down on a yearly basis and what worked one year may no longer be effective.

It is therefore vital that IT security and operations teams truly understand their organization's IT environment and have the agility to move with the threats: knowing what to patch – and when. Otherwise they might as well be patching in the dark (e.g. deploying a patch for a program with vulnerabilities that are not critical while programs with 'Extremely/Highly critical' vulnerabilities remain unpatched).

We all know that manual patching equals complex patching. It puts an immense strain on time and resources and is one of the main reasons why many endpoints remain only partially patched – and thus vulnerable.

The Secunia Package System (SPS) is a cornerstone of the Secunia Corporate Software Inspector's (CSI's) patch configuration functionality stream. The SPS enables IT teams to work smarter, not harder: effective patching of vulnerable software reduces the attack surface and the threats that organizations are exposed too – and frees up valuable time and resources for other projects in the process.

Lock and load your patching strategy

Because every organization is unique, with its own processes, compliance regulations and security procedures to juggle; IT teams need to be able to adapt and scale their patching efforts quickly and efficiently. The security of corporate IT infrastructures depends on this.

The SPS alleviates the strain associated with this challenge by making patch configuration easy and flexible. For example:

The SPS adheres to the reality of corporate IT policies by enabling both scanning and patching – providing a balance between management and operations.

The SPS provides configurable patches out-of-the-box that can be easily customized to support individual environments (e.g. to avoid desktop shortcuts and prompting users to accept an End User License Agreement (EULA) when deploying new updates, or to disable auto-update for a program).
The SPS integrates with third-party patch deployment solutions such as Microsoft WSUS/System Center 2012 Configuration Manager or Altiris, as well as with other complementary Secunia solutions, namely:

- Secunia Vulnerability Intelligence Manager 4.0 (VIM)
- Secunia Personal Software Inspector 3.0 (PSI)
- Secunia PSI for Android

Customization, configuration and control

Specifically, the SPS provides IT teams with the ability to create packages that are capable of performing a wide range of actions; from updating and uninstalling third-party applications, to having the option to change the script and handle multiple files.

When a version of a product has been categorized as insecure (or end of life), and the vendor has a patch available for the insecure product, the SPS page displays a list of products that the Secunia CSI can automatically create an "Update" or "Uninstall" package for.

Establishing the ground rules

Firstly, the SPS package contains predefined settings so that security updates of insecure products can be carried out successfully:

- Applicability criteria/rules are defined (product, minimum and maximum version, installation path, architecture and OS languages) to ensure that the package will target the eligible systems.
- Conveniently, a package can be deployed to ALL systems, yet only the systems that require the package to be installed will receive this 'deployment drop'.

Unleashing the wizard

Secondly, the SPS wizard also allows customers to customize the package to meet their requirements:

- Script execution flows using PowerShell, VBscript or Jscript. Multiple files can be added to the package.
- If localized versions are available, customers can easily choose the desired language for the product. In fact, when future updates of the same product are performed, the language will automatically default to the language previously selected.
- The "SPS Installer Parameters" options – which are dynamic and available for most popular software – allow customers to select options to perform actions including:
- Removing the EULA
- Performing a clean installation
- Disabling automatic updates
- Removing icons from the desktop
- Removing all prior versions and dependencies – regardless of architecture – prior to patching
- Preventing users from granting privileges to applications
- Preventing vendors from collecting anonymous usage statistics

Quality not quantity

Thirdly, the "Minimum Version" option can be used to update older products. Normally a product is updated to its secure version within the same major version. However, customers can alter this behavior by specifying a custom minimum version (the version entered must also be supported by the installer itself as arbitrary values cannot be entered).

Why patching is important

There is plenty of data to support the claim that strategic and proactive patching is an important element of any successful security strategy. Here are some examples:

- The Center for Strategic and International Studies (CSIS) says, "75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching." (1)
- According to Secunia, 84% of the vulnerabilities discovered in the 50 most popular programs in 2012 had a fix available on the day of disclosure. (2)
- Microsoft's Security Intelligence Report reveals that the number of breaches using a particular vulnerability increases exponentially from a few breaches following patch release, to an increase one month later, reaching a peak around 2 months after disclosure. (3)

1: "Raising the Bar for Cybersecurity." James Andrew Lewis. CSIS. 2013. http://csis.org/publication/raising-bar-cybersecurity
2: "Secunia Vulnerability Review 2013." http://secunia.com/vulnerability-review/
3: "Microsoft Security Intelligence Report, Volume 11." http://www.microsoft.com/en-us/download/details.aspx?id=27605

Secunia
Stay Secure

You can get a free trial of the Secunia CSI and test the Secunia Package System (SPS) functionality at **secunia.com/csi**

About Secunia

Secunia is the leading provider of IT security solutions that help businesses and private individuals globally manage and control vulnerability threats and risks across their networks and endpoints.

Secunia plays an important role in the IT security ecosystem, and is the preferred supplier for enterprises and government agencies worldwide, counting Fortune 500 and Global 2000 businesses among our customer base.

Contact

For further information about Secunia's competencies, please contact sales@secunia.com

Stay Secure.

 facebook.com/secunia  gplus.to/secunia  twitter.com/secunia  linkedin.com/company/secunia

Visit us at **secunia.com**