



# WhitePaper

---

## A Strong Foundation for Patch Management

**BUILDING ON SCCM FOR COMPREHENSIVE COVERAGE**

By Nicole Amsler, Vice President of Marketing, Shavlik  
Technologies LLC



## A STRONG FOUNDATION FOR PATCH MANAGEMENT: BUILDING ON SCCM FOR COMPREHENSIVE COVERAGE

For a federal government agency, simply relying on Microsoft's System Center Configuration Manager (SCCM) for patch management is not enough to guarantee network security. Threats are equally – if not more – prevalent through third party (non-Microsoft) applications, such as Adobe, Apple or Java. In fact, according to reports from the National Vulnerability Database, 9 of the top 10 threats in 2010 were not Microsoft applications, but applications from Apple, Adobe and Google. Apple Safari had the highest number of vulnerabilities, followed by Mozilla Firefox and Google Chrome. Other third party applications that ranked within the Top 10 in terms of security flaws included Adobe Flash Player, Reader, Acrobat and Air, as well as Java Runtime and Mozilla SeaMonkey. (See Table 1)

Vulnerabilities in these types of applications continue to be a threat to network security. Qualys, which publishes its Top 10 Vulnerabilities each month, recently included five non-Microsoft applications in its January 2011 Top 10 list. From a recent SANS report, Top Cyber Security Risks, "During the last few years, the number of vulnerabilities being discovered in applications is far greater than the number of vulnerabilities discovered in operating systems." Further, SANS noted that, "On average, major organizations take at least twice as long to patch client-side vulnerabilities as they take to patch operating system vulnerabilities."

**TABLE 1: TOP THREATS OF 2010**

APPLICATION	# of vulnerabilities by severity				SCORE
	TOTAL	HIGH	MEDIUM	LOW	
1. Apple Safari	81	2	71	8	413
2. Mozilla Firefox	44	3	30	11	236
3. Google Chrome	61	1	30	30	206
4. Microsoft Internet Explorer	34	1	30	3	178
5. Adobe Flash Player	34	0	34	0	170
6. Adobe Reader	34	0	34	0	170
7. Java Runtime Environment	28	5	5	18	166
8. Adobe Acrobat	32	0	32	0	160
9. Adobe Air	28	0	28	0	140
10. Mozilla SeaMonkey	20	1	20	5	130
11. Microsoft Office	22	0	22	0	110
12. Mozilla Thunderbird	18	1	14	3	98
13. Adobe Shockwave Player	18	0	18	0	90
14. Oracle Database Server	9	3	0	6	81
15. Microsoft Visio	3	3	0	0	75

Source: National Vulnerability Database

To ensure that all network endpoints are appropriately patched in a timely manner and that compliance guidelines are met, federal government agencies must find a way to expand their patching of third party applications. This is no easy feat, considering that agencies today are faced with tighter budgets and are being required to do more with less.

But adding third party patching is not necessarily impossible given those parameters. Solutions exist today that will enable agencies to enhance security by simply and cost-effectively extending their existing SCCM infrastructure to manage patches for third party applications.

### Doing More... With Less

Federal government agencies must undergo regular audits of their network security, to ensure that all systems and applications are patched properly. The mandates include:

- ▶ Federal Desktop Core Configuration (FDCC), which calls for standardizing the configuration of approximately 300 settings on each of their Windows XP and Vista computers in order to strengthen Federal IT security by reducing opportunities for hackers to access and exploit government computer systems.
- ▶ United States Government Configuration Baseline (USGCB), which evolved from the FDCC, is designed to create security configuration baselines for Windows 7 and Internet Explorer 8 settings that are widely deployed across federal agencies, providing guidance on what should be done to improve and maintain effective configuration settings that focus primarily on security.
- ▶ Information Assurance Vulnerability Alert (IAVA) was developed specifically for the Department of Defense and is an alert system that issues notifications of computer application software or operating system vulnerabilities. Implementation of IAVA policy will help ensure that the appropriate actions are being taken to mitigate vulnerabilities to avoid serious compromises to Defense Department computer system assets that would potentially degrade mission performance.

This document is provided strictly as a guide. No guarantees can be provided or expected.



## A STRONG FOUNDATION FOR PATCH MANAGEMENT: BUILDING ON SCCM FOR COMPREHENSIVE COVERAGE

The SANS™ Institute, a trusted source for computer security research, acknowledged that unpatched client applications are the top security threat facing organizations today. And, while Microsoft software has a reputation of being the most frequently used for cyberattacks, it's actually applications from other organizations that are more problematic.

Waves of targeted e-mail attacks, often called spear phishing, are exploiting client-side vulnerabilities in commonly used programs such as Adobe PDF Reader, Apple QuickTime, Adobe Flash and Microsoft Office. This is currently the primary initial infection vector used to compromise computers that have Internet access. Those same client-side vulnerabilities are exploited by attackers when users visit infected websites.

Brad Arkin, director of product security and privacy at Adobe, told SCMagazineUS.com "The bad guys started out attacking operating systems and services on servers that were exposed. Now those attacks have been moving up the stack. We definitely see the bad guys putting more attention on those third-party products."

Every day new threats are identified and patches must be put in place to maintain the baselines set by these government mandates. But for federal agencies, third party applications can present quite a challenge since the current SCCM infrastructure does not provide a simple way to push these patches out to the hundreds of thousands of endpoints that require updating. The sheer quantity of endpoints that agency IT staff must manage significantly increases the complexity of patch management, and creates the potential that critical endpoints may not be updated, leaving a hole in network security that can be exploited.

Complicating the matter even more is the continued tightening of agency budgets, requiring the IT departments to undertake more, time-consuming security efforts with far fewer resources. This consequence further compromises the effectiveness of an agency's IT department in being able to address more security issues.

### Creating a Robust Infrastructure for Comprehensive Patch Management

Read any computer security report today and it will offer the same conclusion: patching – of both operating systems and applications – is the fundamental effort that any organization should undertake to improve its security profile. In order to minimize exposure to vulnerabilities to the fullest extent, an IT department should patch Microsoft applications and operating systems, legacy and third party applications within SCCM. By doing so, an agency will have a more robust patch management solution.

However, the cost and effort to include these legacy and third party applications in the SCCM infrastructure can be prohibitive. Microsoft provides System Center Updates Publisher (SCUP) so SCCM can deliver updates for third party applications, such as Adobe Reader, Firefox and others. But there is a considerable effort needed in order to implement SCUP. It requires system administrators to dedicate several hours of research to provide the logic for detecting each product and determine if an update is needed.

What these system administrators need is to invest in a solution that can streamline this time-consuming and burdensome task. While agencies have a choice of vendors that deliver tools to assist in this process, there are some general guidelines they should consider when selecting a third party patch management solution for an SCCM infrastructure:

- ▶ **Industry Expertise** – look for a solution that is built and maintained by a team that specializes in patch management.
- ▶ **Expands Security Beyond Microsoft** – because third party applications are some of the biggest threats to network security, any solution should easily scale to manage these third party applications.
- ▶ **Integrates with SCCM** – for simplicity, ease of use and ROI, it is best to find a solution that can run on existing SCCM infrastructure to manage third party applications.
- ▶ **Minimal Cost** – solutions do not have to be expensive to work effectively. Solutions on the

This document is provided strictly as a guide. No guarantees can be provided or expected.



## A STRONG FOUNDATION FOR PATCH MANAGEMENT: BUILDING ON SCCM FOR COMPREHENSIVE COVERAGE

market today can improve the ROI in SCCM and add minimally to the overall cost of patch management.

▶ **Accurate Patch Detection and Deployment**

– a solution provider should have a proven and extendable methodology for identifying and installing missing patches.

▶ **Ease of Implementation** – a solution should

be quickly and easily integrated into the SCCM infrastructure using existing tools and methodologies enabling you to be up and running in 30 minutes or less.

▶ **Single Source of Update Information** – a

solution should provide a catalog that includes update information from multiple vendors in a single file.

▶ **Less Administrative Time and Effort** – a solution

should simplify the extremely difficult and time-consuming effort required to create the detection logic required by SCCM. It should lift this burden from your IT administrators and free them to do more productive work.

▶ **Assists in Fulfilling Compliance Requirements**

– a solution should help a federal agency meet the mandates of programs such as FDCC, USGCB and IAVA, and improve reporting processes to show compliance.

As network security threats increase in number and in the ways they can infiltrate a system, it is imperative for federal government agencies to maintain a strong and effective patch management program as the first, and possibly, best line of defense. By seamlessly integrating third party patch management solutions into existing SCCM infrastructure, federal agencies can be rest assured that all applications in use by their employees – Microsoft, Microsoft legacy and third party applications alike – will not expose critical government networks to security breaches.

This document is provided strictly as a guide. No guarantees can be provided or expected.