



Tackling Third-Party Patches

VMware vCenter Protect Update Catalog Delivers
an Efficient, Effective Way to Extend an Organization's
SCCM Infrastructure

TECHNICAL WHITE PAPER

Companies around the world rely on the Microsoft System Center Configuration Manager (SCCM) for patch management. However, in today's environment, that simply is not enough to bolster network security. Microsoft applications are not the only ones at risk. Third-party applications—such as those from Adobe, Apple and Google—are the cause of most current vulnerabilities. As a result, organizations are forced to dedicate additional resources to ensure comprehensive coverage. Organizations hire additional employees just to manage third-party patches. This isn't always the best use of time or budget, particularly when there are automated solutions that integrate with SCCM. VMware® vCenter™ Protect Update Catalog makes the process less time consuming and is more effective in protecting network security.

Third-Party Threats

There is a common misconception that Microsoft applications are more vulnerable to attacks than other applications. Recent research disproves that theory. Threats are equally—if not more—prevalent through non-Microsoft applications. According to reports from the National Vulnerability Database, 9 of the top 10 threats in 2010 were not Microsoft applications, but applications from companies such as Apple, Adobe and Google. Apple Safari had the highest number of vulnerabilities, followed by Mozilla Firefox and Google Chrome. (See Table 1.)

Application	NUMBER OF VULNERABILITIES BY SEVERITY				Score
	Total	High	Medium	Low	
Apple Safari	81	2	71	8	413
Mozilla Firefox	44	3	30	11	236
Google Chrome	61	1	30	30	205
Microsoft Internet Explorer	34	1	30	3	178
Adobe Flash Player	34	0	34	0	170
Adobe Reader	34	0	34	0	170
Java Runtime Environment	28	5	5	18	168
Adobe Acrobat	32	0	32	0	160
Adobe AIR	28	0	28	0	140
Mozilla SeaMonkey	26	1	20	5	130

	NUMBER OF VULNERABILITIES BY SEVERITY				
	Critical	High	Medium	Low	
Microsoft Office	22	0	22	0	110
Mozilla Thunderbird	18	1	14	3	98
Adobe Shockwave Player	18	0	18	9	90
Oracle Database Server	9	30	0	0	81
Microsoft Visio	3	3	0	0	75
Source: National Vulnerability Database					

Table 1. Top Threats of 2010

Vulnerabilities in these applications continue to threaten network security. Qualys, which publishes its Top 10 Vulnerabilities list each month, included four non-Microsoft applications in its August 2011 Top 10 list. In addition, a recent SANS report entitled Top Cyber Security Risks noted, “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. On average, major organizations take at least twice as long to patch client-side vulnerabilities as they take to patch operating system vulnerabilities.”

Consider the case of a large Fortune 200 company that was plagued with an attack through a third-party application. Because the company was doing all third-party patching manually—on more than 7,000 machines—it took about six days to ensure that the vulnerability was fixed across the entire organization. After this experience, the company sought an automated process that would allow it to be proactive rather than reactive to potential third-party security threats.

To ensure that all network devices are appropriately patched in a timely manner and that compliance guidelines are met, organizations must find a way to expand their patching of third-party applications. This is no easy feat, considering that many companies today are faced with tighter budgets and the IT staff is being required to do more with less.

Achieving effective third-party patching is not necessarily impossible given these challenges. Solutions such as vCenter Protect Update Catalog enable organizations to enhance security by simply and cost-effectively extending the existing SCCM infrastructure to manage third-party patching.

What Is vCenter Protect Update Catalog?

vCenter Protect Update Catalog, designed for both upper mid-market and enterprise needs, facilitates central deployment of non-Microsoft, third-party software patches and updates in a Microsoft Windows environment. With a simple VMware data service to the Microsoft SCCM and System Center Updates Publisher (SCUP) software, vCenter Protect Update Catalog extends Microsoft patch and update management features to hundreds of non-Microsoft applications.

Globally, companies of all sizes distribute software and deploy updates for the latest Microsoft operating systems and applications with SCCM. vCenter Protect Update Catalog leverages Microsoft SCCM patch and update management features to hundreds of other mission-critical applications, including Adobe Reader, Mozilla Firefox, Java applications and legacy Microsoft applications that Microsoft no longer supports.

Maximize Your Investment in SCCM

vCenter Protect Update Catalog extends SCCM beyond Microsoft products using a single workflow. There is no application to install or agent to deploy. Instead, use a single SCCM workflow for deploying updates to Microsoft operating systems, Microsoft applications and non-Microsoft applications.

Reduce Patching Workload

Without vCenter Protect Update Catalog, SCUP requires system administrators to spend hours researching and packaging updates. vCenter Protect Update Catalog provides a catalog with up-to-date information from multiple vendors in a single file that is tested, packaged and ready for deployment. Just select the products to update and let SCCM do the rest according to established policies.

Get Single-Source Updates with Total Coverage

Rather than IT professionals spending hours pushing patches for each publisher, application and version, vCenter Protect Update Catalog handle them all. Get coverage for many third-party applications and Microsoft legacy applications.

vCenter Protect Update Catalog Delivers Business Benefits

Though some IT professionals may argue that it's just as cost-effective to have one or two employees dedicated to managing third-party patching, there are distinct benefits to an automated solution like vCenter Protect Update Catalog:

- **Expertise** – Keeping up with the patches needed for all the products and their versions in use by an organization can be a daunting task, especially for system administrators who may not have the time or background to research all the latest threats and decide which patches are important to their networks. Because the VMware team focuses only on researching the latest patches, it offers a high level of expertise that is almost impossible to match with internal resources.
- **Total coverage** – vCenter Protect Update Catalog extends beyond current Microsoft products to patch third-party applications, including the most frequently attacked, including Adobe, Apple, Mozilla, Google and other applications.
- **Time savings** – Because VMware's experts do the research and package the patches, system administrators can focus on their core responsibilities and be more proactive in their approach to network security. Additionally, by implementing a wide range of patches for Microsoft and non-Microsoft applications, IT is less likely to spend significant time reacting if vulnerabilities are exploited and damage has been done.
- **Ease of use** – vCenter Protect Update Catalog is packaged in an efficient way that makes it easy to deploy and use, without a need to maintain agents on all devices.
- **Maximized ROI in SCCM** – The SCCM infrastructure is used to deploy updates automatically for Microsoft and non-Microsoft applications, all at the same time, with little time investment from a system administrator.

