



The Importance of Patching Non-Microsoft Applications

TECHNICAL WHITE PAPER

The Importance of Patching Non-Microsoft Applications

In the past, organizations patched only Microsoft operating systems. As time passed, the need to patch applications such as Microsoft Office and Internet Explorer became obvious, and organizations responded. However, in recent years, third-party applications have become the primary attack vector for new malware, and organizations haven't been as quick to apply security updates to these applications. Many organizations are at a point where addressing these security threats is no longer optional. What follows is a brief summary of research findings to consider when determining whether an organization can accept the risk of delaying third-party application patching.

Gartner and the Importance of Patching Third-Party Software

"IT organizations must strive for continuous improvement in vulnerability detection and rapid security patch management, especially in often overlooked non-Microsoft components that are Web-facing. Unpatched vulnerabilities are the primary infection method of targeted and mass-propagation threats. Deployment of non-Microsoft patches is often significantly slower and less organized. All Internet-based applications, especially browsers and browser plug-ins (i.e., Adobe and Apple QuickTime), should be a top patching priority."

SANS Institute: Top Cyber Security Risks

Client-Side Software Is Primary Attack Vector

In September 2009, the SANS Institute indicated that unpatched client applications are the number one security threat. "Waves of targeted email attacks, often called spear phishing, are exploiting client-side vulnerabilities in commonly used programs such as Adobe Reader, Apple QuickTime, Adobe Flash and Microsoft Office. This is 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."

Read the full report here: <http://www.sans.org/top-cyber-security-risks/summary.php>

Real-Life HTTP Client-Side Exploitation Example from SANS Institute

"Acme Widgets Corporation suffered a major breach from attackers who were able to compromise their entire internal network infrastructure using two of the most powerful and common attack vectors today: exploitation of client-side software and pass-the-hash attacks against Windows machines."

Learn more about the attack at <http://www.sans.org/top-cyber-security-risks/tutorial.php>

Software Flaws, Delayed Patching

Third-party software programs, such as Adobe Reader and Mozilla Firefox, are known to be responsible for the steady increase in the number of software vulnerabilities affecting computer users.

The total number of vulnerabilities affecting a typical end user is expected to reach close to 800 in 2011, which is an increase of more than 200 percent since 2008. During just the first half of 2011, an average user had seen 90 percent of the total number of bugs that were seen in all of 2010. The precipitous rise in vulnerabilities is attributable to researchers and criminals increasing their focus on third-party applications.

Third-Party Applications Seen as Biggest Security Risk

Contrary to popular belief, Apple leads the pack when it comes to the number of security vulnerabilities, ahead of both Microsoft and Adobe. The number of reported vulnerabilities in major commercial software products is accelerating. Perhaps more important, though, is the fact that third-party applications now account for the vast majority of flaws on most computers. In addition, although Apple products have the highest number of vulnerabilities, Microsoft, Adobe, Mozilla and Oracle are right in the mix, as well.

This alarming development in third-party program vulnerabilities represents an increasing threat to both users and businesses—a threat that continues to be greatly ignored. Users and businesses still perceive operating systems and Microsoft products to be the primary attack vector and largely ignore third-party programs. The perception is that finding ways to secure these products is too complex and time-consuming. Ultimately, this leads to incomplete patch levels of third-party programs, often presenting rewarding and effective targets for criminals.

Top 15 Most Vulnerable Applications

Which were the most vulnerable applications in the first half of 2010? Below are the conclusions drawn from vulnerability data feeds through July 7, 2010 from the National Vulnerability Database (NVD), the U.S. government repository of standards-based vulnerability management data.

According to the NVD, new security vulnerabilities are published at a rate of 16 per day. Vendors are forced to release many security updates to keep their products secure.

APPLICATION	Number of Vulnerabilities by Severity				SCORE
	TOTAL	HI	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
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

Table 1: Top Threats of 2010 Source: National Vulnerability Database

Vulnerable Browsers:

Web browsers are the most targeted applications. They hold the top four places in the NVD's list of vulnerable applications. Other popular targets for hackers are Adobe products, Java Runtime Environment and Microsoft Office.

Discussions about which browser is most secure do not make much sense; they all have new security vulnerabilities. A safe Web browser is one that is used by only a few people and therefore is not popular enough to get attention from hackers. However, on such a browser, many sites will not work simply because most developers test their sites on the most popular browsers.

