



15 Popular Applications with Critical Vulnerabilities

May 2006

<http://www.bit9.com/15apps.html>

Malicious Software is Not Your Biggest Threat

People just can't resist installing their own applications on corporate PCs. Often running outside of IT's knowledge or control, popular applications can present serious risks for enterprise computing environments. Individual users rarely reach the level of discipline required by standard IT practices for patching and upgrading. As a result, the entire corporate desktop environment is littered with vulnerabilities often difficult to track down and even harder to rectify.

Bit9 has compiled this list of applications with known vulnerabilities to help IT departments gain control over their endpoint environments. Each application in this list has the following characteristics:

- Is well-known in the consumer space and frequently downloaded by individuals.
- Is not classified as malicious software by enterprise IT organizations.
- Contains at least one critical vulnerability registered in the U.S. National Institute of Standards and Technology's (NIST) official vulnerability database at <http://nvd.nist.gov>. Every item listed has a severity rating of between 7.0-10.0 (high) on the Common Vulnerability Scoring System (CVSS).
- Relies on the end user, rather than a central administrator, to manually patch or upgrade the software to eliminate the vulnerability, if such a patch exists.

Don't Just Block an Unwanted Installation...

In the past, conventional wisdom held that the best way to protect against these problems was to put users in "least-privileged user account" (LUA) mode. By removing administrative rights, companies were led to believe they could block the execution of unapproved and potentially malicious software. However, this approach has significant drawbacks:

- 1) Some applications don't require administrative approval for installation, and can therefore be installed directly by end users. For example, versions of Firefox exist that can be run off of a USB device, even in LUA mode.
- 2) LUA policies do not affect applications that have already been installed—such applications end up being "grandfathered" into the system. Even worse, the patching process is complicated for these applications because users would not be authorized to install critical updates.
- 3) The deployment of "good" software, such as device drivers or other approved business applications strains IT because temporary administrative rights need to be applied to each PC—often on a case-by-case basis.

...Disable the Entire Application

The best approach for disabling unwanted applications like those presented here is to follow a simple three-step approach that establishes visibility of, knowledge about, and ultimately control over the endpoint environment:

- 1) Understand what is actually running in your organization across your entire desktop and laptop environment—both the known software and the unknown.
- 2) Identify which applications contain known vulnerabilities, are against corporate usage or security policy, or are unwanted for any other reason.
- 3) Permanently ban unwanted software so it cannot run in the organization—leaving you with only approved, appropriately patched software.

The Top Five

- 1) Mozilla Firefox 1.0.7
- 2) Apple iTunes 6.02 & Quicktime 7.0.3
- 3) Skype 1.4
- 4) Adobe Acrobat Reader 7.02, 6.03
- 5) Sun Java Run-Time Environment (JRE) 5.0 Update 3 and 1.4.2_08

Learn more about these 3 must-haves for managing enterprise desktops:

<http://www.bit9.com/cto.html>

■ The Top 15 Vulnerable Applications

Software	Version	Vendor's Solution	Nature of Vulnerabilities	CVE* Number(s)
1 Mozilla Firefox	1.0.7	Patch or upgrade	Multiple vulnerabilities including memory corruption, buffer overflows, errors in garbage collection, and running of arbitrary HTML and Javascript code that in many cases allow the execution of arbitrary code.	CVE-2006-0748 CVE-2006-0749 CVE-2006-1529 CVE-2006-1530 CVE-2006-1790 Many more exist
2 Apple iTunes & Quicktime	iTunes 6.02 / QT 7.0.3	Patch	Several buffer overflows in specially crafted image and video files of various common formats allow remote attackers to cause a denial of service or execute arbitrary code buffer overflows, errors in garbage collection, and running of arbitrary HTML and Javascript code that in many cases allow the execution of arbitrary code.	CVE-2005-2340 CVE-2005-3707 CVE-2005-3708 CVE-2005-3709 Many more exist
3 Skype internet phone	1.4	Patch	A buffer overflow allows a remote attacker to execute arbitrary code when the user clicks on a specially crafted, Skype-specific URL.	CVE-2005-3265
4 Adobe Acrobat Reader	7.02, 6.03	Patch	An unspecified boundary error can allow a remote attacker to cause a denial of service and possibly execute arbitrary code.	CVE-2005-2470
5 Sun Java Run-Time Environment (JRE)	JRE 5.0 Update 3, JRE 1.4.2_08	Patch	Allows remote attackers to escape the Java sandbox and access arbitrary files or execute arbitrary applications via unknown attack vectors.	CVE-2005-3907 CVE-2005-3906 CVE-2005-3905 CVE-2005-3904
6 Macromedia Flash player	7	Patch	Remote attackers can cause denial of service and execute arbitrary code using SWF parameters.	CVE-2005-3591 CVE-2005-2628
7 Winzip compression utility	8.1 SR-1	Upgrade	Allows remote attackers to execute arbitrary code via a MIME archive with certain long MIME parameters.	CVE-2004-0333
8 AOL Instant Messenger	5.5	Upgrade or change registry	Buffer overflow in a specific function handler that allows the remote execution of arbitrary code.	CVE-2004-0636
9 Microsoft Windows/MSN Messenger	5.0	Patch	Buffer overflows related to PNG image processing can be exploited to allow a remote attacker to execute arbitrary code on a user's system.	CVE-2004-0597 CVE-2004-1244
10 Yahoo Instant Messenger	6.0	No fix	Buffer overflow in the Yahoo! Messenger offline mode allows a remote attacker to execute arbitrary code.	CVE-2005-0737
11 Sony / First4 Internet DRM rootkit & uninstaller	All	No fix	Device driver hides files and registry keys. Uninstallation utility to remove this rootkit supports dangerous methods that may be exploited to install arbitrary code on the user's system.	CVE-2005-3650
12 BitDefender anti-virus client	9	Patch	Remote attackers can cause a denial of service and possibly execute arbitrary code via faulty handling of format string specifiers.	CVE-2005-3154
13 Kazaa peer-to-peer client	2.0.2	No fix	A buffer overflow in the FastTrack network code can allow remote execution of arbitrary code.	CVE-2003-0397
14 RealPlayer media player	10	Patch	Boundary errors for DWF files, transfer methods, and file processing can allow remote execution of arbitrary code.	CVE-2005-2922 CVE-2005-2936 CVE-2006-0323 CVE-2006-1370
15 ICQ chat client	2003a	No fix	Mishandling of images, HTML, mail, and other fields allow malicious users to potentially gain system access.	CVE-2003-0235 CVE-2003-0236 CVE-2003-0237

■ Learn More

To learn about how you can gain visibility and control of your enterprise desktops and laptops to streamline IT, enforce policy compliance, and eliminate malicious software; or to download a copy of this document, please visit us at <http://www.bit9.com/15apps.html>.

*CVE stands for Common Vulnerabilities and Exposures

