



The Most Vulnerable Applications—2008 Report

Malicious Software Is Not Your Biggest Threat

■ Seeking the Fully Managed Desktop

As IT professionals, we aim to provide our users with PCs that are secure and well-managed, yet flexible and adaptable. To do this, we rely on a variety of software management and anti-malware tools to provide basic—though limited—control. But, becoming more secure has traditionally meant sacrificing business flexibility, which is almost always an unacceptable choice.

So we manage what we can, accepting that a sizable amount of software evades standard control mechanisms. That's usually software that users install on their own—sometimes for business purposes, other times for personal uses, but always outside of the realm of IT's knowledge. This invisible gray zone contains a mix of business tools, consumer applications, unauthorized software, and the latest and most undetectable malware. But for the sake of business flexibility, we keep the controls dialed down and politely deal with the inevitable mess.

One by-product of the trade-off between flexibility and security are scores of vulnerable applications throughout the environment. They are often difficult to track down and even harder to rectify. More importantly, they can stand in the way of our ability to fully and flexibly control our computing infrastructure. In today's culture of compliance, this lack of control introduces unnecessary security risk and can jeopardize both IT and business operations.

■ Criteria for the Vulnerable Applications List

The applications on this list meet the following criteria.

- 1) Runs on Microsoft Windows.
- 2) Is well-known in the consumer space and frequently downloaded by individuals.
- 3) Is not classified as malicious by enterprise IT organizations or security vendors.
- 4) Contains at least one critical vulnerability that was:
 - a. first reported in January 2008 or after,
 - b. registered in the U.S. National Institute of Standards and Technology's (NIST) official vulnerability database at <http://nvd.nist.gov>, and
 - c. given a severity rating of high (between 7.0-10.0) on the Common Vulnerability Scoring System (CVSS).
- 5) 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.
- 6) The application cannot be automatically and centrally updated via free Enterprise tools such as Microsoft SMS & WSUS.

Note that in most cases, the vendors of these applications have issued patches or other instructions for eliminating the vulnerability. But the nature of these applications is such that the user is responsible for implementing the patch. Enterprise IT organizations can not reliably ensure these patches have been properly applied—if at all—representing an inherent exposure in protecting the enterprise network.

Finally, the applications on the list have been ranked according to the popularity of the application, number and severity of vulnerabilities, and difficulty of detection and/or patching by central IT.

Learn more about what you can do to control vulnerable applications:

www.bit9.com

What You Can Do to Control Vulnerable Applications

Bit9 recommends the following five-step approach to shield and fix vulnerabilities in the application layer.

- 1) Define a full but flexible control policy for applications.
- 2) Understand where the applications are.
- 3) Monitor the Internet for new vulnerabilities.
- 4) Monitor your PCs using software identification services.
- 5) Enforce application controls using Bit9 Parity.

THE GAP IN DESKTOP SOFTWARE MANAGEMENT



2008's Popular Applications with Critical Vulnerabilities

Software	Version	Vendor's Solution	Nature of Vulnerabilities	CVE* Number(s)
1 Mozilla Firefox				
Mozilla Firefox	3.x, 2.x	Vendor Patch	Remote attackers can execute arbitrary code via buffer overflow, malformed URI links, documents, JavaScript and third party tools.	CVE-2008-5052, CVE-2008-5024, CVE-2008-5023, CVE-2008-5022, CVE-2008-5013 CVE-2008-4064, CVE-2008-4063, CVE-2008-4062, CVE-2008-4061, CVE-2008-0016
2 Adobe Flash & Acrobat				
Adobe Flash	10.x before 10.0.12.36 and 9.x before 9.0.151.0	Vendor Patch	Remote attackers can execute arbitrary code via buffer overflow, "input validation issues" and malformed parameters.	CVE-2008-4824, CVE-2008-4473, CVE-2008-3872,
Adobe Acrobat	8.1.2, 8.1.1	Vendor Patch	Arbitrary code execution related to "input validation issue" and malformed PDF objects that trigger memory corruption during parsing.	CVE-2008-4817, CVE-2008-4814, CVE-2008-4813, CVE-2008-4812, CVE-2008-2992 CVE-2008-2641, CVE-2008-2042, CVE-2008-5659, CVE-2008-0655
3 EMC VMware Player, Workstation and other products				
Microsoft Windows Live (MSN) Messenger	ESXi 3.5 or earlier, Workstation 5.5.x, Player 2.0.x & 1.0.x, ACE 2.0.x & 1.0.x	Vendor Patch (Workstation 5.5.6, Player 2.0.3 & 1.0.6, ACE 2.0.1 & 1.0.5)	Privilege escalation via directory traversal vulnerability. ActiveX buffer overflows leading to arbitrary code execution and denial of service.	CVE-2008-4281, CVE-2008-0967, CVE-2008-3892, CVE-2008-3698, CVE-2008-2100 CVE-2008-3691, CVE-2008-3692, CVE-2008-3693, CVE-2008-3694, CVE-2008-3695
4 Sun Java Runtime Environment (JRE)				
Sun Java JDK and JRE	Version 6 Update 6	Upgrade to 7.4	Inability to prevent execution of applets on older JRE release could allow remote attackers to exploit vulnerabilities of these older releases. Buffer overflows allowing creation, deletion and execution of arbitrary files via untrusted applications.	CVE-2008-3115, CVE-2008-3113, CVE-2008-3112, CVE-2008-3111, CVE-2008-3109 CVE-2008-3108, CVE-2008-3107, CVE-2008-1193, CVE-2008-1188, CVE-2008-0657
5 Apple QuickTime, Safari & iTunes				
Apple QuickTime	7.5.5	Vendor Patch	Remote attackers can execute arbitrary code via buffer overflow, or cause a denial of service (heap corruption and application crash) involving malformed media files, media links and third party codecs	CVE-2008-4116, CVE-2008-3635, CVE-2008-3628, CVE-2008-3627, CVE-2008-3625 CVE-2008-3615, CVE-2008-2010, CVE-2008-0778, CVE-2008-0485
Apple Safari	6.0.5.20	Vendor Patch	Buffer overflow resulting in arbitrary code execution and denial of service involving JavaScript arrays that trigger memory corruption and crafted images, related to improper handling of color spaces.	CVE-2008-3623, CVE-2008-2307 CVE-2008-2306
Apple iTunes	3.2, 3.1.2	Vendor Patch	Remote Improper update verification allows man-in-the-middle attacks to execute arbitrary code via a Trojan horse update.	CVE-2008-3434
6 Symantec				
Symantec Norton Products (all flavors 2006 to 2008)	2.7.0.1	Vendor Patch	Stack-based buffer overflow in the AutoFix Support Tool ActiveX lead to arbitrary code execution.	CVE-2008-0312
7 Trend Micro				
Trend Micro OfficeScan	8.0 SP1 before build 2439 and 8.0 SP1 Patch 1 before build 3087	Vendor Patch	Stack-based buffer overflow allowing remote attackers to execute arbitrary code.	CVE-2008-3862, CVE-2008-4402, CVE-2008-2437, SVE-2008-3364
8 Citrix Products				
Citrix Products	Deterministic Network Enhancer (DNE) 2.21.7.233 through 3.21.7.17464, Access Gateway 4.5.7, Presentation Server 4.5	Vendor Patch	Privilege escalation in DNE via specially crafted device interface requests affects Cisco VPN Client, Blue Coat WinProxy, SafeNet SoftRemote and HighAssurance Remote. Search path vulnerability, authentication bypass and buffer overflow lead to arbitrary code execution.	CVE-2008-5121, CVE-2008-3485, CVE-2008-2528, CVE-2008-0356

Software	Version	Vendor's Solution	Nature of Vulnerabilities	CVE* Number(s)
9 Aurigma, Lycos Aurigma Image Uploader, Lycos FileUploader	4.6.17.0, 4.5.70.0, 4.5.126.0	Vendor Patch	Remote attackers can perform remote code execution via long extended image information. Aurigma ActiveX is used by Facebook PhotoUploader and MySpace MySpaceUploader.	CVE-2008-0660, CVE-2008-0659, CVE-2008-0443
10 Skype Skype	3.6.0.248	Vendor Patch	Improper check of dangerous extensions allows user-assisted remote attackers to bypass warning dialogs. Cross-zone scripting vulnerability allows remote attackers to inject script via IE web control.	CVE-2008-2545, CVE-2008-1805, CVE-2008-0454
11 Yahoo! Assistant Yahoo! Assistant	3.6.	Vendor Patch	Remote attackers can execute arbitrary code via memory corruption.	CVE-2008-2111
12 Microsoft Windows Live (MSN) Messenger Microsoft Windows Live (MSN) Messenger	4.7 & 5.1	Vendor Patch	Remote attackers are allowed to control the Messenger application, "change state," obtain contact information and establish audio or video connections without notification.	CVE-2008-0082

*CVE stands for Common Vulnerabilities and Exposures

What You Can Do To Control Vulnerable Applications

Bit9 recommends the following five-step approach to shield and fix these vulnerabilities in the application layer.

1) *Define a full but flexible control policy for applications.*

Answer questions such as: What applications will we authorize users to install on their own?
If a vulnerability is found, what is the proper recourse?

2) *Understand where the applications are.*

An unknown vulnerability could jeopardize sensitive data—and your company's reputation—if a laptop connects to a public wi-fi spot.

3) *Monitor the Internet for new vulnerabilities.*

Excellent resources are available at sites such as the National Vulnerability Database (<http://nvd.nist.gov>), the SANS Institute (<http://www.sans.org>).

4) *Monitor your PCs using software identification services.*

Services such as FileAdvisor (<http://fileadvisor.bit9.com>) let you look up any file and identify its product, publisher, security rating, and more

5) *Enforce application controls using Bit9 Parity.*

Bit9 Parity controls what applications can and can not run by helping you build and automatically maintain a whitelist of authorized software. Vulnerable applications can be easily found and banned, filling the gap in endpoint protection.

- Identify and stop non-business applications on your Windows desktops—call Bit9 today: +1.617.393.7400 or visit us at www.bit9.com.



Bit9, Inc.
266 Second Ave.
Waltham, MA 02451
p: +1 617.393.7400
f: +1 617.393.7499
www.bit9.com