Report: Top Vulnerable Applications – 2010

Continuous Endpoint Monitoring

Malicious cyber attacks are happening with greater frequency, leveraging common applications and social media vehicles that are part of everyday lives. Consumers and enterprise IT are becoming more vigilant and taking more precautions, but it still may not be enough.

This report provides a wake-up call that users and companies need to be even more vigilant and proactive about knowing what's on their computers and other endpoints—smart phones, PDAs, USBs, attachments—and protecting those endpoints. Hackers go where the people are and these vulnerable applications are some of the most popular and prevalent ones out there today—used to moved business, ecommerce and social media.

It's interesting to note that Apple applications are growing in number on this list. There was a time when Apple customers were secure in the knowledge that they "couldn't" be hacked and "couldn't" get a virus. The reality is the Apple footprint wasn't big enough for malicious attackers to focus on. Now, as a byproduct of its success, both in the consumer market and with its growing footprint in the enterprise, Apple is also now in the sights of attackers.

The applications on this list meet the following criteria:

- Is an end-user/consumer application and not an enterprise-only application like a server or router.
- Is not classified as malicious by enterprise IT organizations or security vendors.
- Contains at least one critical vulnerability that was:
  - Reported between January 1, 2010 through October 21, 2010.
  - Registered in the NIST database at http://nvd.nist.gov, and given a severity rating of high (between 7.0-10.0) on the Common Vulnerability Scoring System (CVSS).

Note: In most cases, the vendors of these applications have issued patches or other instructions for eliminating the vulnerability.

What You Can Do to Control Vulnerable Applications

Bit9 recommends the following six-step approach to shield and protect your endpoints:

1. Define a baseline by discovering and mapping all the existing applications.
2. Create a full but flexible control policy for applications on endpoints.
3. Employ forensics to identify, validate and understand the reputation of software on endpoints.
4. Monitor your PCs using continuous monitoring and identification services.
5. Monitor the Internet for new vulnerabilities.
6. Enforce application controls using Application Whitelisting.

Software	Nature of Vulnerabilities—Examples[1]	CVE Identifiers[2]
Adobe Reader and Acrobat	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	CVE-2010-3658 CVE-2010-3619 CVE-2010-2206 CVE-2010-0199 CVE-2010-3632 CVE-2010-2890 CVE-2010-2205 CVE-2010-0198 CVE-2010-3631 CVE-2010-2889 CVE-2010-2204 CVE-2010-0197 CVE-2010-3630 CVE-2010-2888 CVE-2010-2202 CVE-2010-0196 CVE-2010-3629 CVE-2010-2887 CVE-2010-2201 CVE-2010-0195 CVE-2010-3628 CVE-2010-2884 CVE-2010-2168 CVE-2010-0194 CVE-2010-3627 CVE-2010-2883 CVE-2010-1295 CVE-2010-0193 CVE-2010-3626 CVE-2010-2862 CVE-2010-1285 CVE-2010-0192 CVE-2010-3625 CVE-2010-2212 CVE-2010-1297 CVE-2010-0191 CVE-2010-3624 CVE-2010-2211 CVE-2010-1278 CVE-2010-1241 CVE-2010-3623 CVE-2010-2210 CVE-2010-0204 CVE-2010-1240 CVE-2010-3622 CVE-2010-2209 CVE-2010-0203 CVE-2010-0188 CVE-2010-3621 CVE-2010-2208 CVE-2010-0202 CVE-2010-3620 CVE-2010-2207 CVE-2010-0201
Adobe Flash	Untrusted search path vulnerability in Adobe Flash Player 10.1.82.76, and possibly other versions, allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse dwmapi.dll that is located in the same folder as a file that is processed by Flash. Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	CVE-2010-3976 CVE-2010-3975 CVE-2010-2216 CVE-2010-2214 CVE-2010-2213 CVE-2010-0209 CVE-2010-0379 CVE-2010-0378
Adobe Shockwave	Adobe Shockwave Player before 11.5.8.612 does not properly validate a count value in a Director movie, which allows remote attackers to cause a denial of service (heap memory corruption) or execute arbitrary code via a crafted movie, related to IML32X.dll and DIRAPIX.dll. Adobe Shockwave Player before 11.5.8.612 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.	CVE-2010-2874 CVE-2010-2873 CVE-2010-2863 CVE-2010-1283 CVE-2010-2882 CVE-2010-2872 CVE-2010-1291 CVE-2010-1281 CVE-2010-2881 CVE-2010-2871 CVE-2010-1290 CVE-2010-1280 CVE-2010-2880 CVE-2010-2870 CVE-2010-1289 CVE-2010-0987 CVE-2010-2879 CVE-2010-2869 CVE-2010-1288 CVE-2010-0986 CVE-2010-2878 CVE-2010-2868 CVE-2010-1287 CVE-2010-0130 CVE-2010-2877 CVE-2010-2867 CVE-2010-1286 CVE-2010-0129 CVE-2010-2876 CVE-2010-2866 CVE-2010-1284 CVE-2010-0127 CVE-2010-2875 CVE-2010-2864 CVE-2010-1292
Apple QuickTime	Apple QuickTime before 7.6.6 on Windows allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted BMP image.	CVE-2010-1818 CVE-2010-0529 CVE-2010-1799 CVE-2010-0528 CVE-2010-0536 CVE-2010-0527
Apple Safari	WebKit in Apple Safari 4.x before 4.1.2 and 5.x before 5.0.2 does not properly validate floating-point data, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted HTML document. Use-after-free vulnerability in WebKit in Apple Safari before 5.0 on Mac OS X 10.5 through 10.6 and Windows, and before 4.1 on Mac OS X 10.4, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors involving DOM Range objects.	CVE-2010-1807 CVE-2010-1774 CVE-2010-1404 CVE-2010-1177 CVE-2010-1806 CVE-2010-1771 CVE-2010-1403 CVE-2010-1176 CVE-2010-1793 CVE-2010-1770 CVE-2010-1402 CVE-2010-1120 CVE-2010-1792 CVE-2010-1761 CVE-2010-1401 CVE-2010-1119 CVE-2010-1791 CVE-2010-1759 CVE-2010-1400 CVE-2010-0054 CVE-2010-1790 CVE-2010-1758 CVE-2010-1399 CVE-2010-0053 CVE-2010-1789 CVE-2010-1419 CVE-2010-1398 CVE-2010-0052 CVE-2010-1788 CVE-2010-1750 CVE-2010-1397 CVE-2010-0050 CVE-2010-1787 CVE-2010-1749 CVE-2010-1396 CVE-2010-0049 CVE-2010-1786 CVE-2010-1417 CVE-2010-1392 CVE-2010-0048 CVE-2010-1785 CVE-2010-1415 CVE-2010-1385 CVE-2010-0047 CVE-2010-1784 CVE-2010-1414 CVE-2010-1939 CVE-2010-0046 CVE-2010-1783 CVE-2010-1412 CVE-2010-1181 CVE-2010-0045 CVE-2010-1782 CVE-2010-1410 CVE-2010-1180 CVE-2010-0043 CVE-2010-1780 CVE-2010-1405 CVE-2010-1179 CVE-2010-0040

[1] All the vulnerabilities are not listed here due to space constraints.

[2] CVE Identifiers are unique, common identifiers for publicly known information security vulnerabilities. More information can be found at: http://nvd.nist.gov/.

continued on page 3

Software	Nature of Vulnerabilities—Examples[1]	CVE Identifiers[2]
Apple WebKit	Use-after-free vulnerability in WebKit in Apple iOS before 4.1 on the iPhone and iPod touch allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors involving scrollbars. WebKit in Apple iOS before 4.1 on the iPhone and iPod touch allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via vectors involving form menus.	CVE-2010-1815 CVE-2010-1814 CVE-2010-1813 CVE-2010-1812 CVE-2010-1781 CVE-2010-1760 CVE-2010-1386 CVE-2010-0659 CVE-2010-0647
Google Chrome	Google Chrome before 7.0.517.41 does not properly handle element maps, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "stale elements." Use-after-free vulnerability in WebKit, as used in Google Chrome before 6.0.472.59, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to nested SVG elements.	CVE-2010-4042 CVE-2010-4040 CVE-2010-4039 CVE-2010-4035 CVE-2010-4034 CVE-2010-3730 CVE-2010-3729 CVE-2010-1822 CVE-2010-1825 CVE-2010-1824 CVE-2010-1823 CVE-2010-1773 CVE-2010-1772 CVE-2010-3416 CVE-2010-3415 CVE-2010-3414 CVE-2010-3412 CVE-2010-3258 CVE-2010-3257 CVE-2010-3255 CVE-2010-3254 CVE-2010-3253 CVE-2010-3252 CVE-2010-3249 CVE-2010-3120 CVE-2010-3119 CVE-2010-3117 CVE-2010-3116 CVE-2010-3115 CVE-2010-3114 CVE-2010-3113 CVE-2010-3112 CVE-2010-3111 CVE-2010-2903 CVE-2010-2902 CVE-2010-2901 CVE-2010-2900 CVE-2010-2898 CVE-2010-2897 CVE-2010-2651 CVE-2010-2650 CVE-2010-2648 CVE-2010-2647 CVE-2010-2646 CVE-2010-2302 CVE-2010-2300 CVE-2010-2299 CVE-2010-2298 CVE-2010-2297 CVE-2010-2296 CVE-2010-2110 CVE-2010-2109 CVE-2010-2108 CVE-2010-2107 CVE-2010-2106 CVE-2010-2105 CVE-2010-1665 CVE-2010-1663 CVE-2010-1506 CVE-2010-1505 CVE-2010-1502 CVE-2010-1500 CVE-2010-1237 CVE-2010-1236 CVE-2010-1234 CVE-2010-1233 CVE-2010-1231 CVE-2010-1230 CVE-2010-1229 CVE-2010-1228 CVE-2010-0658 CVE-2010-0657 CVE-2010-0655 CVE-2010-0649 CVE-2010-0646 CVE-2010-0645
Microsoft Internet Explorer	Microsoft Internet Explorer 6 through 8 does not properly handle objects in memory in certain circumstances involving use of Microsoft Word to read Word documents, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability."	CVE-2010-3331 CVE-2010-3329 CVE-2010-3328 CVE-2010-3326 CVE-2010-2560 CVE-2010-2559 CVE-2010-2558 CVE-2010-2557 CVE-2010-2556 CVE-2010-1262 CVE-2010-1261 CVE-2010-1260 CVE-2010-1259 CVE-2010-0807 CVE-2010-0805 CVE-2010-0492 CVE-2010-0491 CVE-2010-0490 CVE-2010-0489 CVE-2010-0267 CVE-2010-1175 CVE-2010-1118 CVE-2010-1117 CVE-2010-0806 CVE-2010-0555 CVE-2010-0248 CVE-2010-0247 CVE-2010-0246 CVE-2010-0245 CVE-2010-0244 CVE-2010-0027 CVE-2010-0249
Microsoft Office	Microsoft Excel 2002 SP3, Office 2004 and 2008 for Mac, and Open XML File Format Converter for Mac do not properly validate record information, which allows remote attackers to execute arbitrary code via a crafted Excel document, aka "Ghost Record Type Parsing Vulnerability." Microsoft Word 2002 SP3 and 2003 SP3, Office 2004 for Mac, and Word Viewer do not properly handle a malformed record during parsing of a Word document, which allows remote attackers to execute arbitrary code via a crafted document that triggers memory corruption, aka "Word Parsing Vulnerability."	CVE-2010-3242 CVE-2010-3241 CVE-2010-3240 CVE-2010-3239 CVE-2010-3238 CVE-2010-3237 CVE-2010-3236 CVE-2010-3235 CVE-2010-3234 CVE-2010-3233 CVE-2010-3232 CVE-2010-3231 CVE-2010-3230 CVE-2010-3221 CVE-2010-3220 CVE-2010-3216 CVE-2010-3215 CVE-2010-3214 CVE-2010-2750 CVE-2010-2748 CVE-2010-2747 CVE-2010-2738 CVE-2010-3142 CVE-2010-3141 CVE-2010-2562 CVE-2010-1902 CVE-2010-1901 CVE-2010-1900 CVE-2010-1263 CVE-2010-1253 CVE-2010-1252 CVE-2010-1251 CVE-2010-1250 CVE-2010-1249 CVE-2010-1248 CVE-2010-1247 CVE-2010-1246 CVE-2010-1245 CVE-2010-0824 CVE-2010-0823 CVE-2010-0822 CVE-2010-0821 CVE-2010-0815 CVE-2010-0264 CVE-2010-0263 CVE-2010-0262 CVE-2010-0261 CVE-2010-0260 CVE-2010-0258 CVE-2010-0257 CVE-2010-0243 CVE-2010-0034 CVE-2010-0033 CVE-2010-0032 CVE-2010-0031 CVE-2010-0030 CVE-2010-0029

[1] All the vulnerabilities are not listed here due to space constraints.

[2] CVE Identifiers are unique, common identifiers for publicly known information security vulnerabilities. More information can be found at: http://nvd.nist.gov/.

continued on page 4

Software	Nature of Vulnerabilities—Examples[1]	CVE Identifiers[2]
Mozilla Firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.5.x before 3.5.14 and 3.6.x before 3.6.11, Thunderbird before 3.0.9 and 3.1.x before 3.1.5, and SeaMonkey before 2.0.9 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors. Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 do not properly restrict the role of property changes in triggering XUL tree removal, which allows remote attackers to cause a denial of service (deleted memory access and application crash) or possibly execute arbitrary code by setting unspecified properties.	CVE-2010-3183 CVE-2010-3180 CVE-2010-3179 CVE-2010-3176 CVE-2010-3175 CVE-2010-3174 CVE-2010-3173 CVE-2010-3169 CVE-2010-3168 CVE-2010-3167 CVE-2010-3166 CVE-2010-2770 CVE-2010-2767 CVE-2010-2766 CVE-2010-2765 CVE-2010-2760 CVE-2010-3131 CVE-2010-2753 CVE-2010-2752 CVE-2010-1214 CVE-2010-1212 CVE-2010-1211 CVE-2010-1209 CVE-2010-1208 CVE-2010-2755 CVE-2010-1203 CVE-2010-1202 CVE-2010-1201 CVE-2010-1200 CVE-2010-1199 CVE-2010-1198 CVE-2010-1196 CVE-2010-0183 CVE-2010-1988 CVE-2010-1585 CVE-2010-0179 CVE-2010-0178 CVE-2010-0177 CVE-2010-0176 CVE-2010-0175 CVE-2010-0174 CVE-2010-0173 CVE-2010-1122 CVE-2010-1121 CVE-2010-0168 CVE-2010-0167 CVE-2010-0165 CVE-2010-0164 CVE-2010-1028 CVE-2010-0160 CVE-2010-0159
Opera	Opera before 10.63 does not properly restrict web script in unspecified circumstances involving reloads and redirects, which allows remote attackers to spoof the Address Bar, conduct cross-site scripting (XSS) attacks, and possibly execute arbitrary code by leveraging the ability of a script to interact with a web page from (1) a different domain or (2) a different security context.	CVE-2010-4045 CVE-2010-2666 CVE-2010-2657 CVE-2010-2421 CVE-2010-1728 CVE-2010-1349
Real Networks Real Player	Array index error in RealNetworks RealPlayer 11.0 through 11.1 and RealPlayer SP 1.0 through 1.0.1 allows remote attackers to execute arbitrary code via malformed sample data in a RealMedia .IVR file, related to a "malformed IVR pointer index" issue. Unspecified vulnerability in RealNetworks RealPlayer 11.0 through 11.1 allows attackers to bypass intended access restrictions on files via unknown vectors.	CVE-2010-3751 CVE-2010-3750 CVE-2010-3749 CVE-2010-3748 CVE-2010-3747 CVE-2010-2998 CVE-2010-2578 CVE-2010-3002 CVE-2010-3001 CVE-2010-3000 CVE-2010-2996 CVE-2010-0120 CVE-2010-0117 CVE-2010-0116
Sun Java Development Kit	Unspecified vulnerability in the Sound component in Oracle Java SE and Java for Business 6 Update 21, 5.0 Update 25, 1.4.2_27, and 1.3.1_28 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	CVE-2010-3572 CVE-2010-3571 CVE-2010-3570 CVE-2010-3569 CVE-2010-3568 CVE-2010-3567 CVE-2010-3566 CVE-2010-3565 CVE-2010-3563 CVE-2010-3562 CVE-2010-3561 CVE-2010-3559 CVE-2010-3558 CVE-2010-3556 CVE-2010-3555 CVE-2010-3554 CVE-2010-3553 CVE-2010-3552 CVE-2010-3550 CVE-2010-0886 CVE-2010-1423 CVE-2010-0850 CVE-2010-0849 CVE-2010-0848 CVE-2010-0847 CVE-2010-0846 CVE-2010-0844 CVE-2010-0843 CVE-2010-0842 CVE-2010-0841 CVE-2010-0840 CVE-2010-0839 CVE-2010-0838 CVE-2010-0837 CVE-2010-0094 CVE-2010-0087

[1] All the vulnerabilities are not listed here due to space constraints.

[2] CVE Identifiers are unique, common identifiers for publicly known information security vulnerabilities. More information can be found at: http://nvd.nist.gov/.

What You Can Do to Control Vulnerable Applications

Bit9 recommends the following six-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. **Identify, validate and understand the reputation of software on endpoints.** Bit9 Cyber Forensics Services leverages Bit9's Global Software Registry, the world's largest and most complete authority on software, to triage an entire computer in minutes, dramatically reducing the time required to perform comprehensive Cyber Forensics Investigations.
4. **Monitor the Internet for new vulnerabilities.** Excellent resources are available at sites such at the National Vulnerability Database (http://nvd.nist.gov) and the SANS Institute (www.sans.org).
5. **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.
6. **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.

Bit9

266 Second Avenue Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.bit9.com