

# OPERATING SYSTEMS SECURITY

YEAR 2007 VULNERABILITY REPORT



By  
Ajit Gaddam

## Table of Contents

<b>Executive Summary</b> .....	<b>3</b>
<b>Introduction</b> .....	<b>4</b>
<b>Measuring Operating System Security</b> .....	<b>4</b>
Days of Risk as a Metric .....	5
<b>Quantitative Metrics Description &amp; Assumptions</b> .....	<b>5</b>
Time Period.....	6
Mitre CVE List .....	6
<b>Operating Systems Security</b>	
Windows Vista.....	7
Windows XP.....	8
Comparison of Windows Vista & Windows XP .....	9
RedHat Enterprise Linux 4 WS Reduced.....	10
Ubuntu 6.06 LTS.....	12
Mac OS X 10.4 .....	14
<b>Side-by-Side Comparison of Operating System Security</b>	
Vulnerability Analysis.....	15
Days of Risk Analysis.....	16
<b>Web Browser Security Analysis</b> .....	<b>17</b>
<b>Conclusion</b> .....	<b>19</b>
<b>Appendix</b>	
Appendix A (Vulnerability Information & Data).....	20
Frequently Asked Questions.....	36
Sources .....	37

## EXECUTIVE SUMMARY

Classic OS protection techniques are no longer able to protect against the constant evolving threat landscape to any IT infrastructure. Increasingly untrustworthy software residing on top of an OS, including active web code and remotely exploited applications, means that it is no longer sufficient to protect users from each other.

This paper analyzes the vulnerability disclosures and security updates during the year 2007 for Windows Vista Operating System when compared to its predecessor, Windows XP, along with other modern Client Operating Systems Red Hat, Ubuntu and Apple Mac OS X.

The results of this analysis based on the *Vulnerability Count* Metric and *Days of Risk* suggest that **Windows Vista is the most secure Operating System when compared to the other leading Desktop Operating Systems for the year 2007** based on its lower vulnerability profile. Windows Vista is also significantly easier to administer for IT Security of various corporations as well as individual users based on the number of Security Bulletins and updates it issues besides the excellent security support provided through Microsoft [TechNet Security Center](#).

With the vulnerability and risk data available, I also wanted to tackle the topic of Browser security. The analysis reveals that **Firefox 2.x on Ubuntu platform was the most secure browser for the year 2007** in terms of the lowest Days of Risk and vulnerability profile.

While these results represent only the vulnerability dimension of security risk, they do provide insight into the aspects of security quality that are under the control of the vendors – code security quality and security response. These metrics however, must be considered in combination with several other important qualitative factors when choosing a platform based upon security maintenance and likelihood of a security breach in your environment.

Beyond patches and vulnerabilities, there are “softer” qualities of security that are difficult to quantify but undeniably impact deployed security. Qualities like security lifecycle support, bulletin descriptiveness, default security features and the like all have a direct impact on deployed role security.

**Note:** This report is an update to the previously published [Windows Vista One Year Vulnerability Report by Jeff Jones](#)<sup>1</sup>, a VP at Microsoft, who concluded that Windows Vista is more secure by analyzing vulnerability data of Windows Vista and other Operating Systems based on the first year of their operation. However, as Jeff admits, this kind of first year analysis may be good to evaluate the security practices and product development methodologies of a vendor more than measure the security of an Operating system. This paper expands on his findings while following a similar structure used in Jeff’s report presenting a deeper level of analysis and comparison of the modern workstation Operating Systems using the entire 2007 vulnerability and risk data which would more accurately reflect the “present security state” of these different Operating Systems.

---

<sup>1</sup> <http://blogs.technet.com/security/archive/2008/01/23/download-windows-vista-one-year-vulnerability-report.aspx>

## INTRODUCTION

With Operating System Security, there is a need for preventing the unauthorized reading or modification of data, or the unauthorized use of resources. Traditionally, protection has been based on the idea of protecting users from each other. The operating system and other programs authenticate a user, and the user is the basis of protection policies. Applications a user runs on his behalf are assumed to perform according to their specifications.

The rise of the Internet, however, has drastically reduced the trust that can be placed in software running on our Operating Systems. First, a tremendous amount of active content can be run simply by loading a Web page or reading an e-mail lowering the barriers to entry. Also, the use of spyware and adware, disguised as legitimate software, is on the rise. Also, we are going to see local applications interpreting more and more remote content, increasing the likelihood that a malicious user can exploit vulnerabilities to take control of the program, the operating system and finally the machine itself.

Operating System vendors use the term “secure” to describe the state of their products. However, the reality is that how secure a system really is lies in the *implementation* of the Operating System itself.

## MEASURING OPERATING SYSTEM SECURITY

How does one measure the security of an Operating System or for that matter, measure Information Security? After all, the common mantra seems to be “You can’t manage what you can’t measure” and “what gets measured gets done”. So, by measuring the number of vulnerabilities and their severity, can we determine how secure an Operating System is? Can these metrics predict future risk trends? What do these numbers actually tell us? And if these numbers are lower this year from last year or their first year, can the vendor claim success about providing enhanced security?

I tried to approach this Operating System Security Metrics based on an ISSA paper on Seven Myths about Information Security Metrics<sup>2</sup>. **Measuring anything makes it easier to drive improvements but measuring the wrong things leads to improving the wrong things. The hard part is not measurement *per se* but figuring out the suite of parameters that need altering and to measure and work on them all, acknowledging that many of the measures are interdependent. Information Security is a complex field with ramifications throughout the organization. It is unrealistic to expect to find a few simple measures.**

That being said, since Operating System security is all about reducing risk and process outputs such as better audit reports, reduction in virus incidents, reduction in vulnerabilities are all worthwhile sources of metrics and I will be using the vulnerability count and Days of Risk to provide a vulnerability analysis which could be incorporated with other factors such as various kinds of controls and Defense in Depth measures to provide for reduced risk for different kinds of environments whether corporate or home.

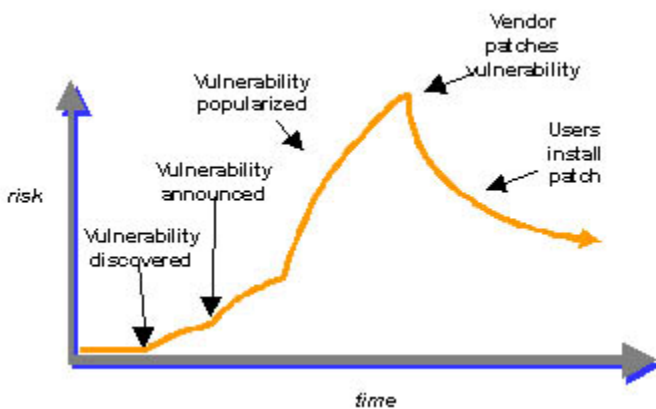
---

<sup>2</sup> <https://www.issa.org/Members/Log-In.php?d=Library%2FJournals%2F2006%2FJuly%2FHinson+-Seven+Myths.pdf>

## DAYS OF RISK AS A METRIC

Days-of-Risk (DoR) is a measurement of the time period of greatly increased risk from when a vulnerability has been publicly disclosed (and thus known and available to millions of script-kiddies and other malicious attackers) until a vendor patch is available to close the vulnerability.

I like the [vulnerability lifecycle chart](#) from Bruce Schneier's September 2000 Crypto-Gram Newsletter, because it illustrates key points where risk might increase dramatically. Essentially, days-of-risk as it is commonly used is the time from "Vulnerability announced" until the "Vendor patches vulnerability" points on Schneier's chart.



I believe the potential usefulness of days-of-risk (and related variations) as a metric is to monitor and make improvements to drive vendors to optimize towards reduced user risk. Though days-of-risk is most obviously related to the vendor maintenance and security response process, it is worth noting that there are actions that can be taken to help reduce the total number of vulnerabilities and move towards reducing the opportunities for vulnerability discovery.<sup>3</sup>

## QUANTITATIVE METRICS DESCRIPTION & ASSUMPTIONS

Any comparisons of various Operating System security measurement historically was made using quantitative and readily available data and counts of "security advisories or bulletins" issued by the different vendors.

While these counts are popular, vendors control how many vulnerabilities are addressed by a single security advisory. So to compensate the inherent weakness of just using raw bulletin counts, I will be using Days of Risk and a role based approach of measuring security of these different operating systems using a likely deployed client configuration environment. So, this analysis will take advantage of Linux ability to create and deploy a minimum set of components, a security advantage it has over Windows.

<sup>3</sup> [http://blogs.csoonline.com/basic\\_guide\\_to\\_days\\_of\\_risk](http://blogs.csoonline.com/basic_guide_to_days_of_risk)

The overall vulnerability information can be obtained from public bug reporting lists and from Microsoft TechNet reports. The list of these sources is listed in Appendix B. The following is the set of conditions that was used to gather the vulnerability information and patch information

- i. I install only patches and fixes released by Microsoft. Similarly for Red Hat and the other Operating Systems, I only install patches released by the vendor.
- ii. The “first public” date for a vulnerability is the date at which the vulnerability was first released on a public list or a web site (Bugtraq, Red Hat, Microsoft, Full-disclosure, Security Focus, k-otik) devoted to security, or a publicly accessible list of bugs or problems posted to the home site of a package or its mailing list.
- iii. Dates of patches are based on the release date for the distribution of interest.
- iv. Release dates for a vulnerability patch or fix are specific to a distribution/architecture. If a fix for a component (ex: libpng) is released on 01/01/2007 for a certain Linux distribution (ex: Gentoo Linux) and a fix for the same issue is released for Red Hat on 01/10/2007, the release date for the fix on Red Hat will be 01/10/2007. This is not applicable for the Windows platform.
- v. For past issues, the release date for a patch is the first published vendor report that includes the patch for the applicable platform for which the patch fully fixed the vulnerability. If the patch had to be re-issued to address some portion of the security issue, the later date is used.

## Time Period

The methodology used for this comparison could be applied to any fixed time period for comparisons. For Server 2003 analysis, vulnerabilities disclosed earlier than 2007 will be used if any only if Microsoft has released a fix for these issues in 2007. Similarly, a vulnerability announced in 2007 but fixed in 2008 will not be considered.

When considering the relative security of Windows Server 2003, it is important not just to consider *what* is installed, but also *how* it is installed. Thus, the context in which a role is deployed is important when considering the long-term security of a solution.

## Mitre CVE List

In this analysis, I use the CVE or CAN identifier of vulnerability. CVE stands for Common Vulnerabilities and Exposures and provides a standardized taxonomy for all publicly known vulnerabilities and exposures. In this analysis, I refer to a vulnerability as distinct if it has its own CVE number. In rare instances, it is possible for a vulnerability to not have been assigned a CVE number. In such a case, this vulnerability would not be considered for this analysis.

## WINDOWS VISTA – YEAR 2007

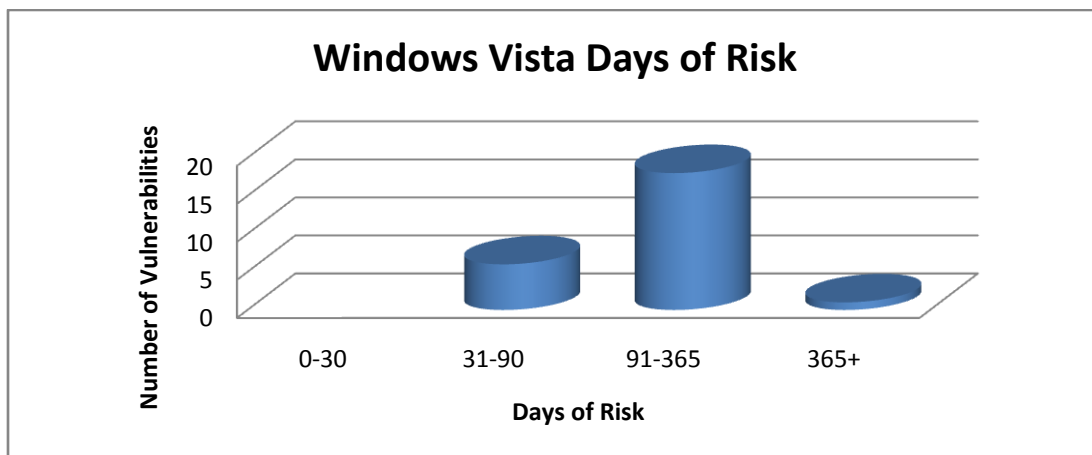
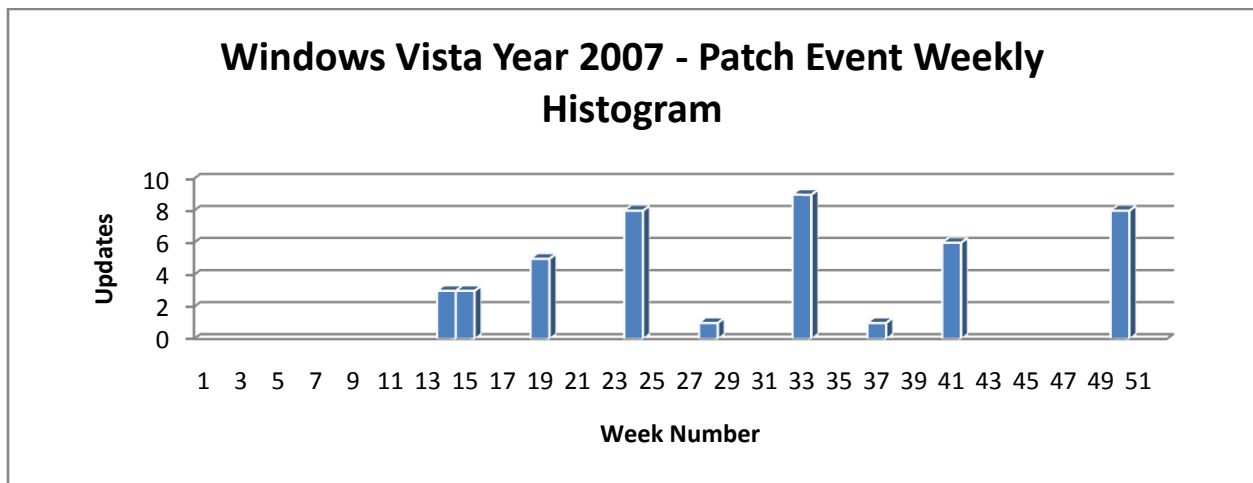
With the previous Windows Operating Systems, they never supported the principle of least privilege even in their discretionary access control systems. While there was some concept of a completely privileged security domain and a completely unprivileged security domain, Microsoft introduced many security measures with its latest flagship Operating System, Windows Vista.

Looking at security updates for Windows Vista during the year 2007, Microsoft released a total of 22 Security Bulletins and corresponding patches in the year 2007 affecting components of Windows Vista. These fixed 44 different vulnerabilities. For Windows Vista, the average Days of Risk for these vulnerabilities was 163.69 days.

Excluded: Development (.Net Frameworks)

Included: Browser (Internet Explorer 7), Windows Media Player 11, DirectX 10.0

To get a better feel for the frequency and impact of these security updates for administrators throughout the year, I've also charted a histogram of Patch Events on a graph of the first fifty-two weeks of availability. There were ten, and no week had more than one security update.



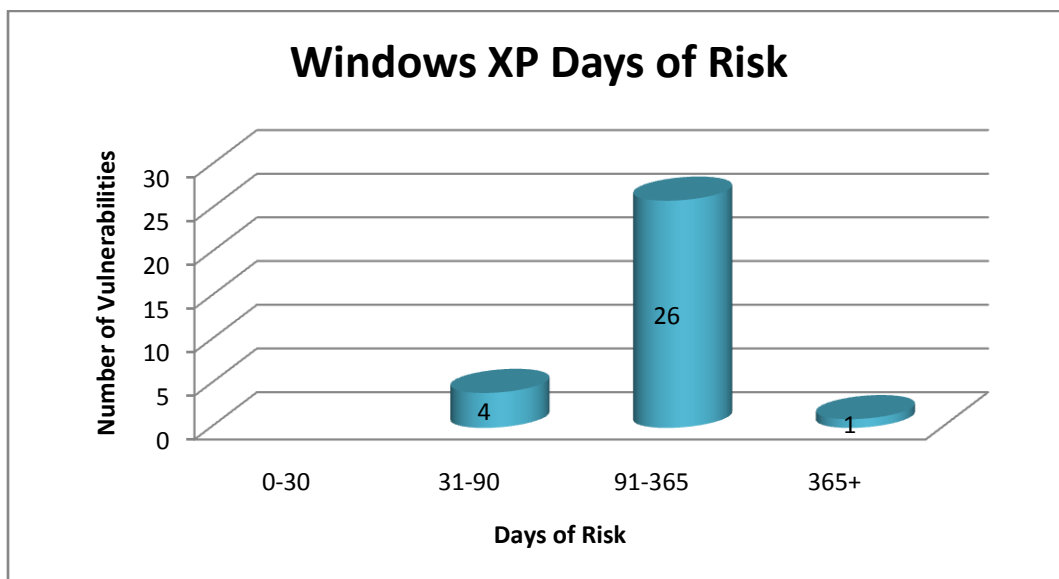
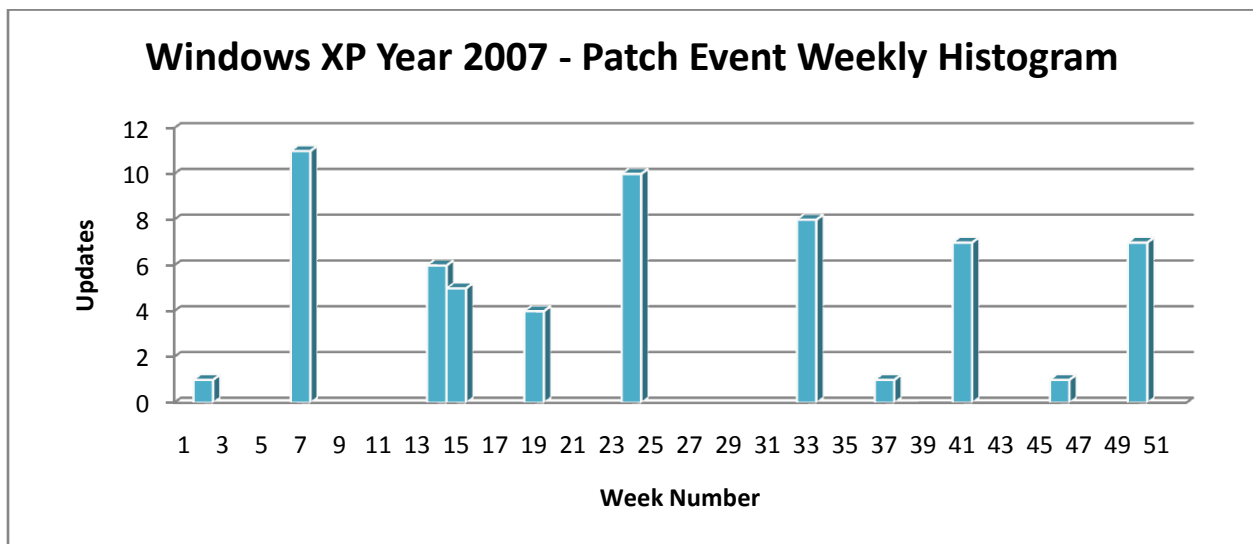
## WINDOWS XP – YEAR 2007

Next, let's take a similar look for Windows XP in the year 2007. Windows XP shipped on October 25<sup>th</sup> 2001 and had a while to mature as a secure Operating System especially after the release of Service Pack 2.

Excluded: Development (.Net frameworks), Web (IIS)

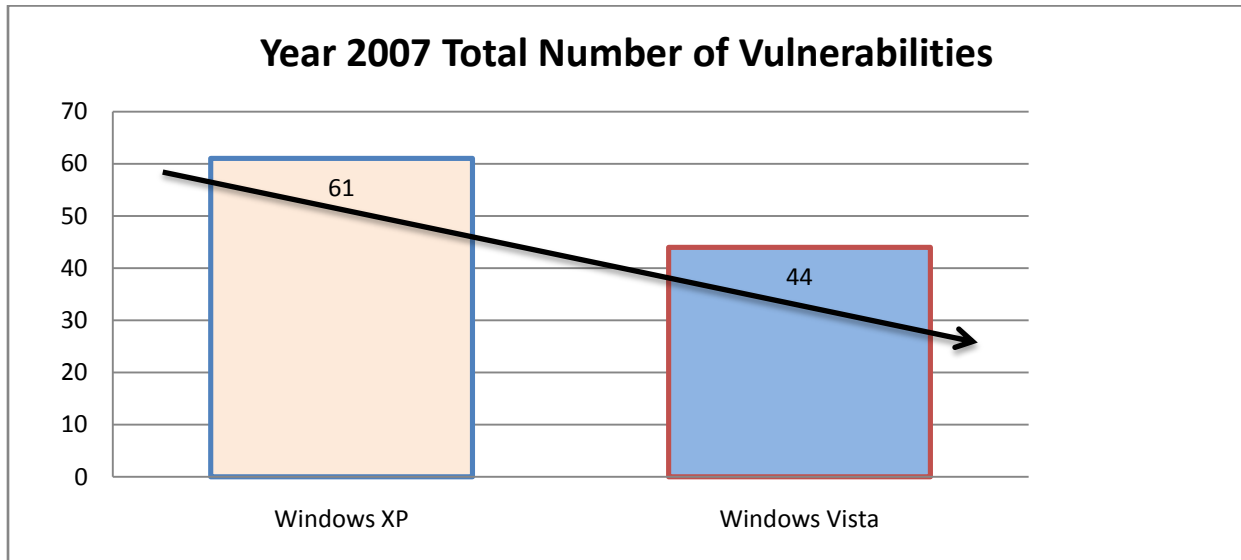
Included: The version of Windows XP considered is Windows XP Professional SP2 with Internet Explorer 6 with Service Pack 1 (IE) , Windows Media Player 10 (WMP) and DirectX 9.0

Windows XP in year 2007 had 61 different vulnerabilities which were patched over 39 different security bulletins. The average Days of Risk for these Windows XP vulnerabilities was 161.52 days. Charted out as Patch Events, Figure 2 shows what year 2007 looked like for Security Administrators for Windows XP



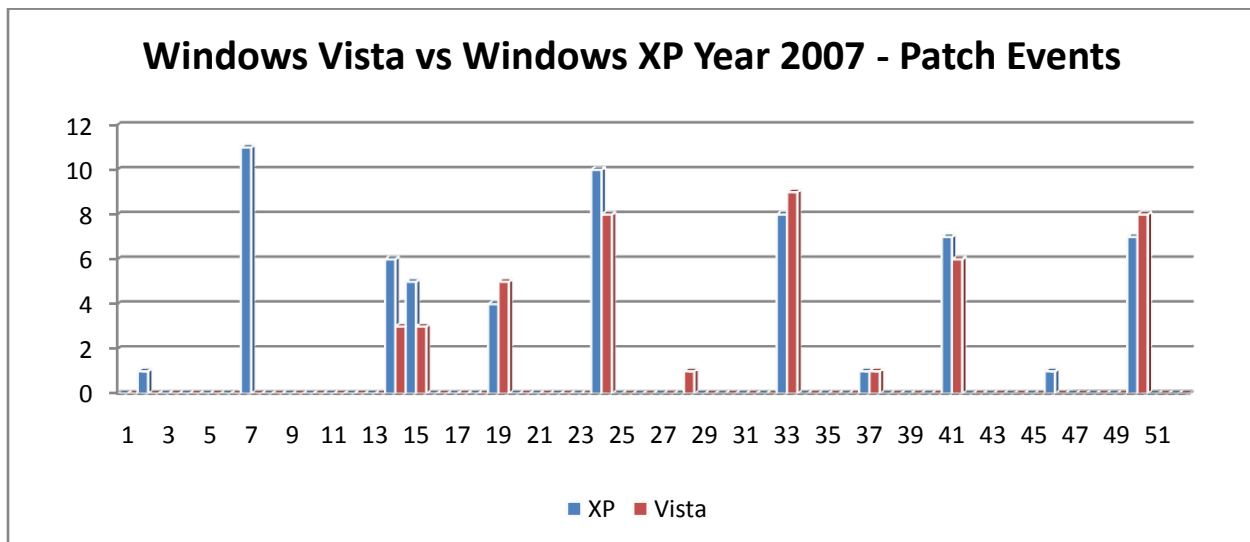
SIDE – BY – SIDE COMPARISON of WINDOWS VISTA and WINDOWS XP

With the basic analysis completed for Windows Vista and Windows XP, we now have enough information to compare them. First, let's look at a chart that shows the total number of vulnerabilities fixed for Windows Vista and Windows XP side-by-side.



We can see a reduction in vulnerabilities from Windows XP (61) to Windows Vista (44) in the year 2007.

Next, let us examine the impact that security updates had for administrators by looking at Patch Events in Figure 4. Windows Vista's 44 security updates occurred across 9 Patch Events in 9 different weeks in the year 2007. Windows XP's 61 security updates occurred across 12 Patch Events in 12 different weeks in the year 2007.



Graphed out visually, it is easy to see that there is reduced work to manage security risk with Windows Vista in 2007 when compared to Windows XP in the year 2007.

Here is a summary table of the key data discussed above.

Metric	Windows Vista	Windows XP
Vulnerabilities fixed	44	61
Security Updates	21	39
Patch Events	9	12
Weeks with at least 1 Patch Event	9	12

#### WINDOWS VISTA VS OTHER OPERATING SYSTEMS

Comparing the same products which Jeff Jones used, I will be using other workstation products that offered long-term support options – Red Hat, Ubuntu and Mac OS X 10. Again, the comparison will be made with the flagship version that has been running for the whole of 2007.

#### RED HAT ENTERPRISE LINUX

Red Hat shipped Red Hat Enterprise Linux 5 in March 2007. However, it will not be included in this analysis since I am looking for a full year worth data. So, the version of Red Hat I will examine is Red Hat Enterprise Linux 4 Workstation (rhel4ws).

Like Jeff Jones, I will not count the vulnerabilities for all the components for the product that Red Hat ships and supports as Red Hat Enterprise Linux 4 WS. To accommodate this idea, I will only use a reduced set of components in comparisons.

#### RHEL4WS – REDUCED COMPONENT SET

I install a rhel4ws computer and:

- I excluded any component that is not installed by default, which includes all optional “server” components that ship with rhel4ws.
- I additionally excluded *text-internet*, *graphics* (the gimp stuff) and *office* (OpenOffice) and *Development Tools* (gcc, etc) installation groups.
- I also used the rpm command to list out all packages that get installed and used that package list to filter vulnerabilities for inclusion.

This process results in a Gnome – windows workstation that includes standard system management tools, Firefox for browsing, sound and video support, but excludes all server packages, as well as OpenOffice and other optional stuff that a Windows system wouldn't have by default.

**Excluded Components:** Development (gcc, gdb, qt, libpng, Ruby, Perl, Python, php), Office Apps (Open Office, Thunderbird, Mailman, SquirrelMail, FetchMail, SpamAssassin, Mutt), Database (mysql, postgresql), Utilities (SeaMonkey, xpdf, gpdf, kpdf, TeTeX,CUPS), Graphics (GIMP, gtk2, ImageMagick), Security (GnuPG, Wireshark, Tcpdump, OpenSSH), Web (Apache, OpenLDAP, W3C libwww, htdig, Squid), Browsers (Opera, ELinks, Konqueror), Entertainment (HelixPlayer, FLAC)

**Included Components:** Browser (Firefox), Mail (SpamAssassin, Mutt), Messaging (GnomeMeeting), Security (Kerberos, shadowutils, SASL), Utilities (BusyBox, util-linux, unzip, GIMP)

This reduced rhel4ws build is then examined for comparison:

- During the year 2007, Red Hat issued 67 Security Advisories affecting the rhel4ws reduced set of components on 43 different days during 31 different weeks. If limited to only those security advisories containing issues rated Critical or Important by Red Hat, there were 29 Security Advisories released on 26 different days during 21 different weeks.
- Red Hat fixed 160 different vulnerabilities affecting the reduced rhel4ws set of components. If limited to those rated Critical or Important by Red Hat, the number drops down to 114 vulnerabilities.

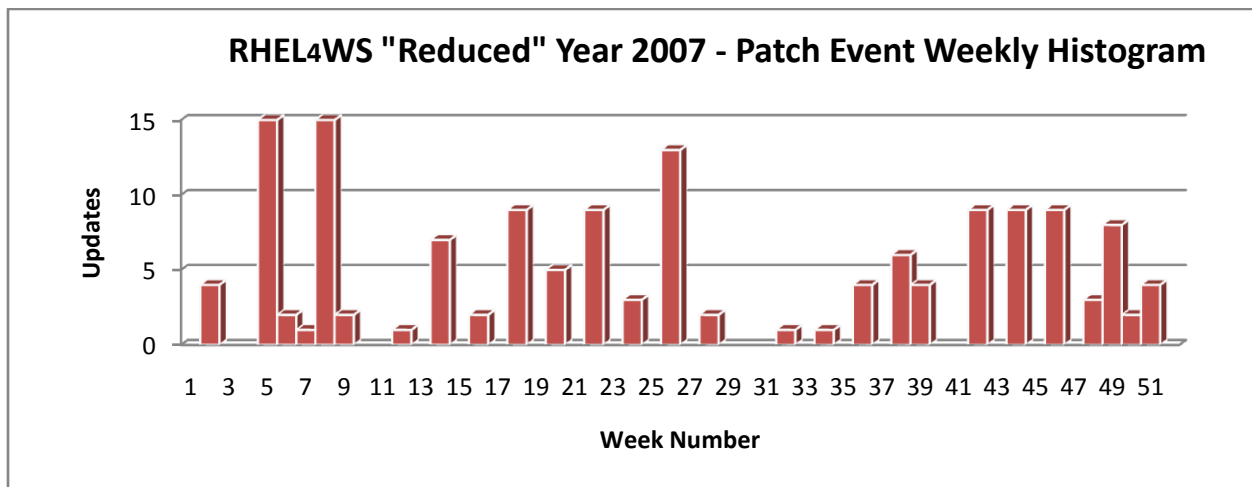
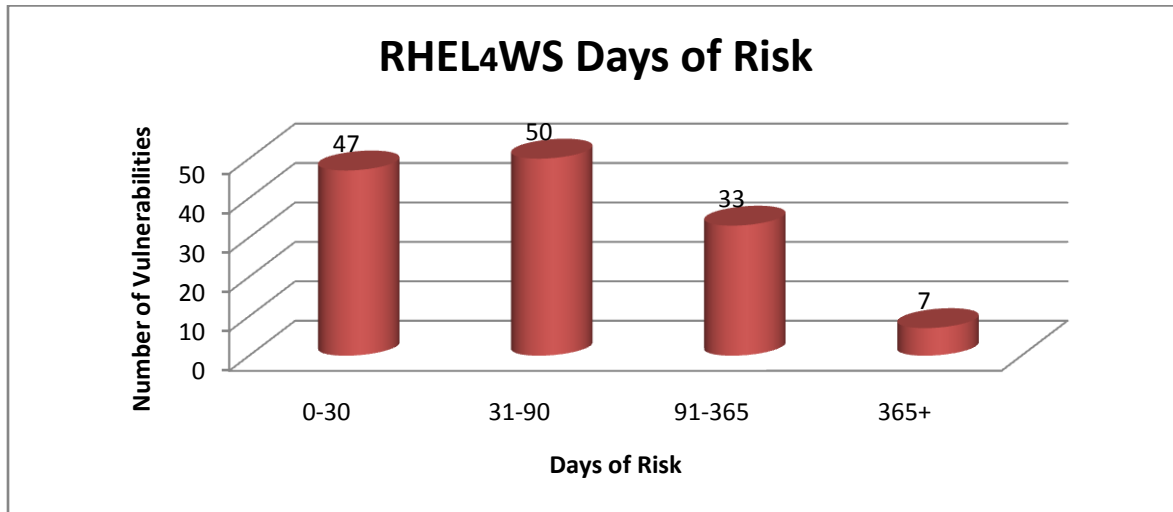


Figure : RHEL4 WS Reduced Year 2007 – Patch Event Weekly Histogram



#### UBUNTU 6.06 LTS

Ubuntu releases new versions every six months, and supports those releases for 18 months with daily security fixes and patches to critical bugs. The most recent version, Ubuntu 7.10 (Gutsy Gibbon), was released on 18 October 2007.

There are also Long Term Support (LTS) releases, which have three years support for the desktop version and five years for the server version. The most recent major LTS version, Ubuntu 6.06 (Dapper Drake), was released on June 1, 2006. The next major LTS version will be 8.04 (Hardy Heron), scheduled for release in April 2008.

So, with a full year worth vulnerability data to analyze and with Long Term Support, I will be looking at Ubuntu 6.06 LTS for this analysis.

#### UBUNTU 6.06 LTS – REDUCED COMPONENT SET

Similar to the component set reduction I did for RHEL4WS, for this analysis of Ubuntu 6.06 LTS, I will exclude components that do not have comparable functionality shipping with Windows Vista or Windows XP.

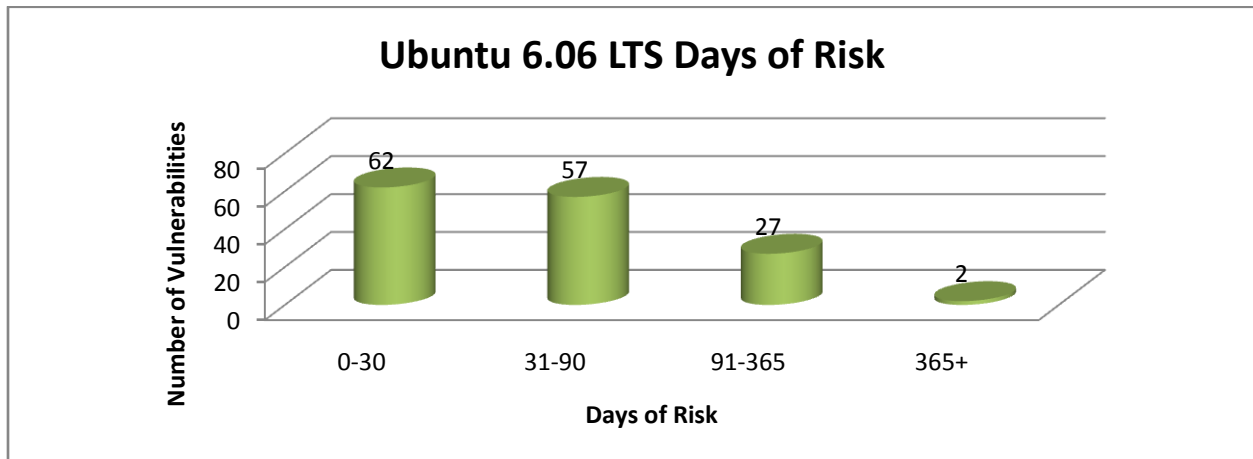
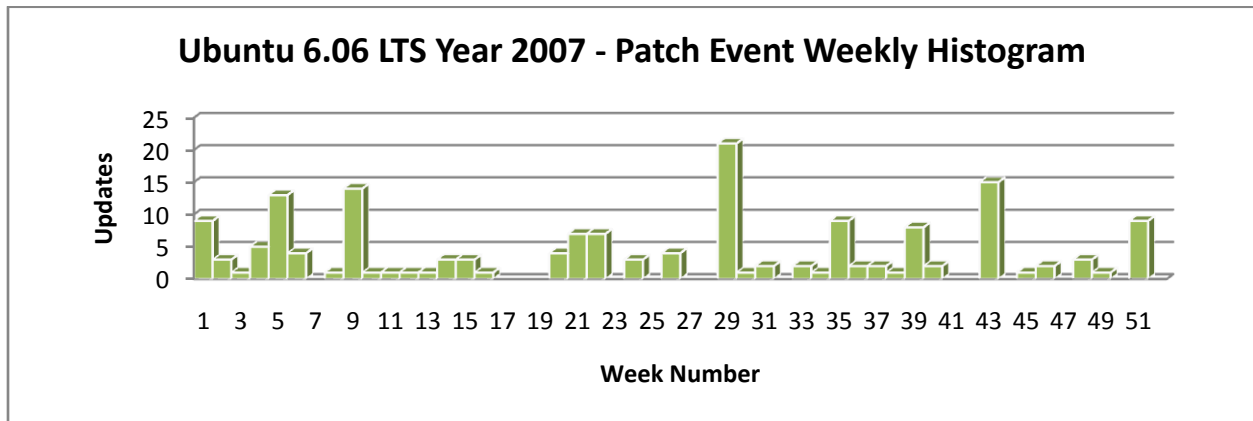
Ubuntu is pretty good. For example, with their advisory USN – 511 – 1, they released a patch for a Kerberos Vulnerability. However, this only reduced the scope of the vulnerability, without fully solving it. Three days later, they announce and release a full fix. It is hard to fault someone who are rushing to get a patch out which at least tried to mitigate the risk their customers are facing at the earliest. Another example is if a patch breaks something such as USN – 544 -1 which fixed vulnerabilities in Samba. However, some fixes introduced regression in smbfs mounts. Ubuntu released a patch fixing this regression later the same day.

Excluded Components: Browser (w3m, Konqueror, ELinks), Office/Productivity (OpenOffice, Thunderbird, koffice, fetchmail, libwpd, Tomboy), Messaging (ksirc, Ekiga), Applications (kword, KTorrent, Inkscape, Gnome, rdesktop, racoon, Poppler, Ghostscript, VMWare, TeTeX, CUPS), Database (postgreSQL), Web (Squid, MoinMoin, NAS, snmpd, pptpd, libpng, dovecot, Apache, Jasper), Development (PHP, Python, libgd2, Qt, vim, Tk, PCRE, Perl, Mono,pwlib), Security (Enigmail, tcpdump, GnuPG, Nagios), Entertainment (XMMS, FLAC), Graphics (GIMP, ImageMagick, Cairo, GD Library), Other Libraries (t1lib)

Included Components: Browser (Firefox), Utilities (Emacs), Entertainment (xine,libsndfile), Security (Kerberos)

This reduced Ubuntu build is then examined for comparison:

- During the year 2007, Ubuntu issued 65 security advisories covering the reduced desktop build of Ubuntu 6.06. These fixes were released on 54 different days during the year 2007 in 37 different weeks
- During the year 2007, Ubuntu fixed 168 vulnerabilities affecting the reduced Ubuntu desktop set of components.



APPLE MAC OS X V 10.4

Mac OS X v10.4 "Tiger" was released on April 29, 2005. Among the new features, Tiger introduced Spotlight, Dashboard, Smart Folders, updated Mail program with Smart Mailboxes, QuickTime 7, Safari 2, Automator, VoiceOver, Core Image and Core Video.

On January 10, 2006, Apple released the first Intel-based Macs along with the 10.4.4 update to Tiger. This operating system functioned identically on the PowerPC-based Macs and the new Intel-based machines, with the exception of the Intel release dropping support for the Classic environment.

For this analysis, I will be reviewing the Mac OS X 10.4.8 and beyond. This version update was released on September 29<sup>th</sup> 2006 and has the full 2007 vulnerability data to analyze. Apple announced the Mac OS X 10.4.9 on March 13<sup>th</sup> 2007 and shipped the next generation of OS X, the Mac OS X v 10.5 "Leopard" on 10/26/2007 which does not have a one-year track record data for this analysis.

Apple does not have a good Security Bulletin naming system. For example, there are multiple instances of the same Security Bulletin number describing different security bulletins addressing different vulnerabilities on different products.

Excluded: Any Beta products, Server related, iTunes, Xcode, Java, Airport, CUPS, Development (Perl, Python, Ruby, XQuery), Applications/Software (Shockwave, Flash, PDFKit, VPN, VideoConference, Ftpd, OpenSSH)

Included: Safari (Browser), Multimedia (QuickTime), iChat, iPhoto

- During the year 2007, Apple released 9 Security Updates (15 Security Updates if QuickTime is included) affecting Mac OS X 10.4.
- These updates fixed a total of 154 vulnerabilities in shipping components of Mac OS X 10.4
- This number of vulnerabilities increases to 187 if QuickTime is included in this count of security vulnerabilities.

Below is the patch event chart for Mac OS X 10.4 for the year 2007

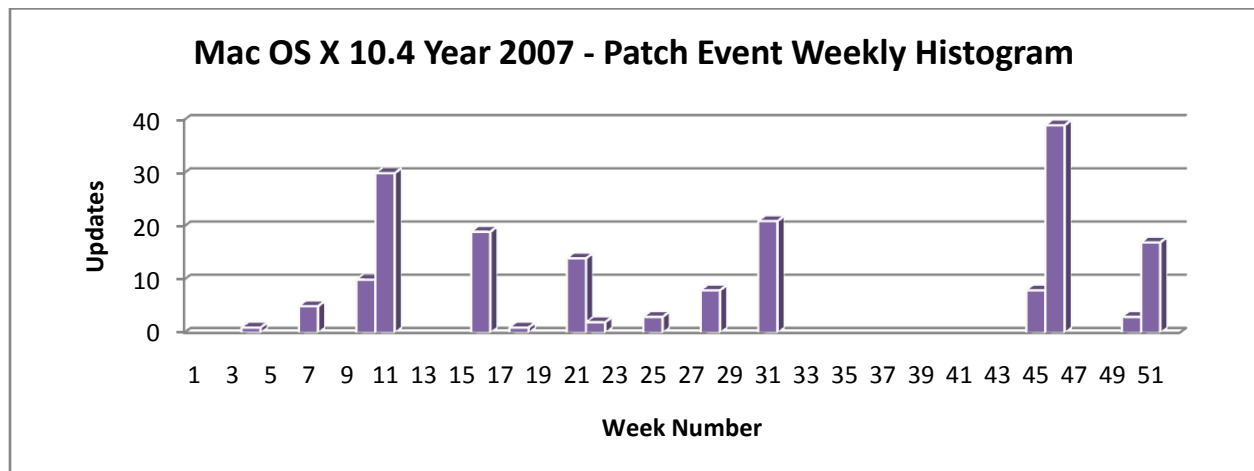
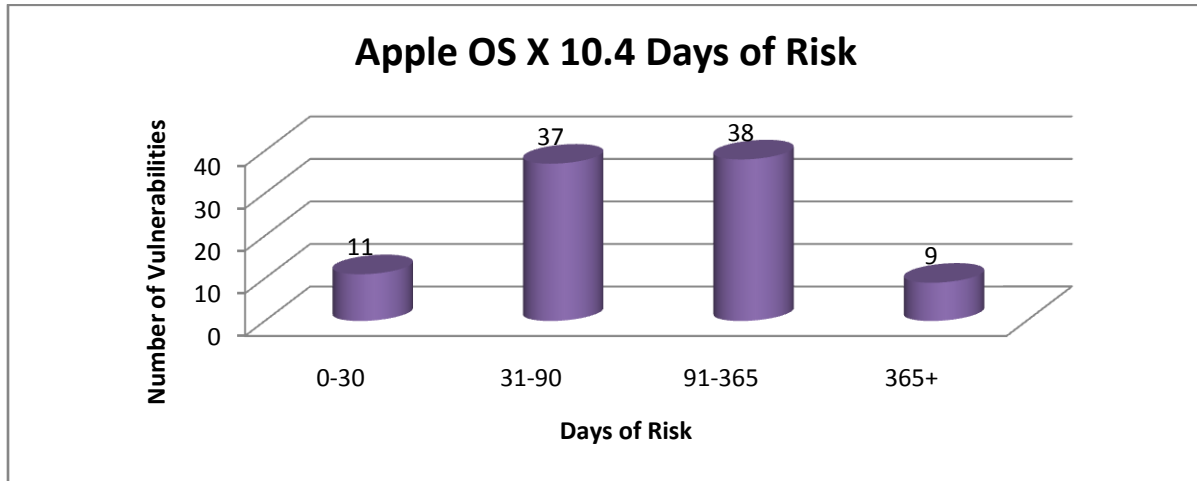


Figure : Mac OS X 10.4 Year 2007 – Patch Events



**SIDE – BY – SIDE COMPARISON**

With the basic analysis completed for Windows Vista and other industry products, we now have enough information to compare them. First let's look at a chart that examines the impact that security updates had for administrators by looking at Patch Events.

*Note: For Apple OS X, from now on, any analysis would include the numbers which include QuickTime vulnerabilities.*

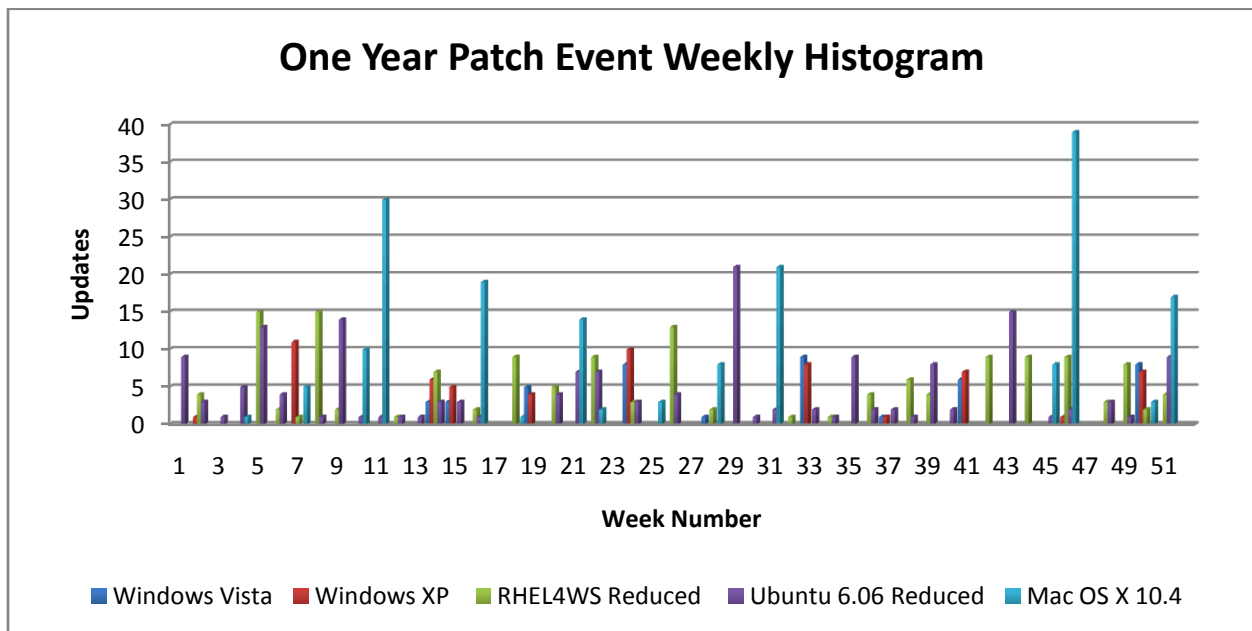
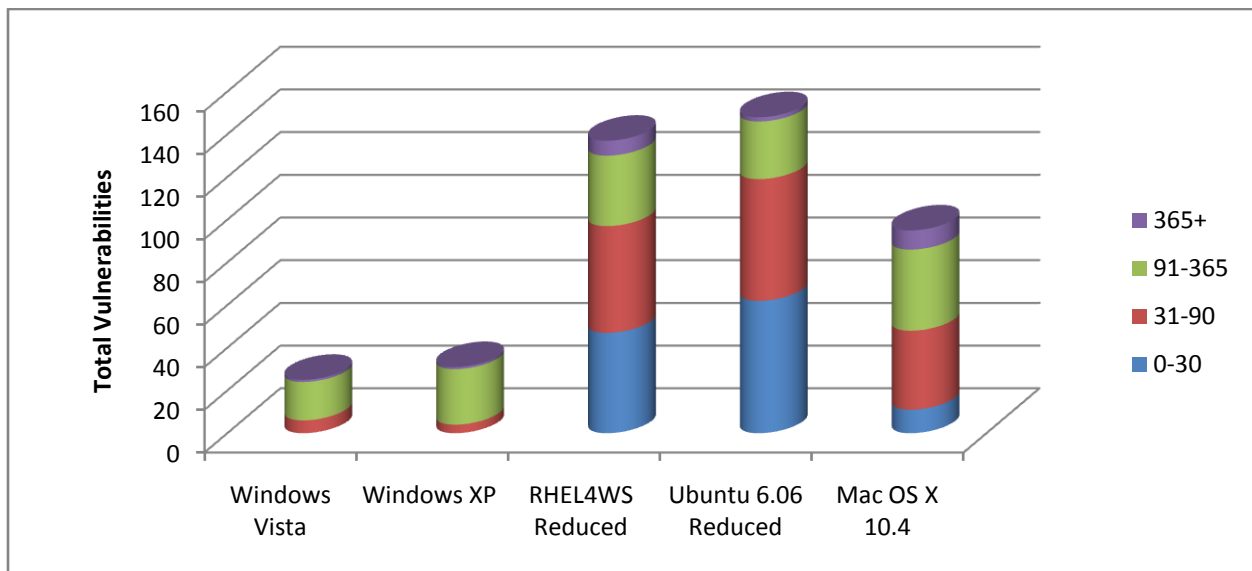


Figure : Patch Event Histogram for all the major Desktop Operating Systems for year 2007

Graphed out visually in this case, it is hard to see anything. So, Table below is a bit more informative for comparison.

Metric	Windows Vista	Windows XP	Red Hat rhel4ws Reduced	Ubuntu 6.06 LTS reduced	Mac OS X 10.4
Vulnerabilities Fixed	42	66	160	168	187
Security Updates	21	39	67	65	15
Patch Events	9	12	43	54	19
Weeks with at least 1 Patch Event	9	12	31	37	15

#### Days of Risk for all Operating Systems



#Days	Windows Vista	Windows XP	RHEL4WS	Ubuntu 6.06	Mac OS X 10.4
0-30			47	62	11
31-90	6	4	50	57	37
91-365	18	26	33	27	38
365+	1	1	7	2	9

## WEB BROWSER SECURITY

All the current stable web browsers in use today, Internet Explorer 6, Internet Explorer 7, Firefox 2.x, Safari 3.x are not fully equipped to deal with all the malware on today's Internet.

The next generation of browsers such as Internet Explorer 8 and Firefox 3 plan to do a tighter integration with anti-malware and anti-fraud mechanisms such as IE8 incorporating Windows Vista's protected mode and IE8 using a sandbox mechanism and malware blockers.

But despite those moves, vulnerabilities and malicious hacker attacks that use the browser as the entry point to desktops continue to rise as indicated by the current number of browser exploits. In hacking contests to hack three different notebooks running Mac OS X, Ubuntu and Vista, network attacks against all three failed the first day. However, when the contest was opened up to include browser exploits, Mac OS X failed in 2 minutes<sup>4</sup>, Windows Vista running IE7 went next and then Ubuntu running Firefox all get hacked.

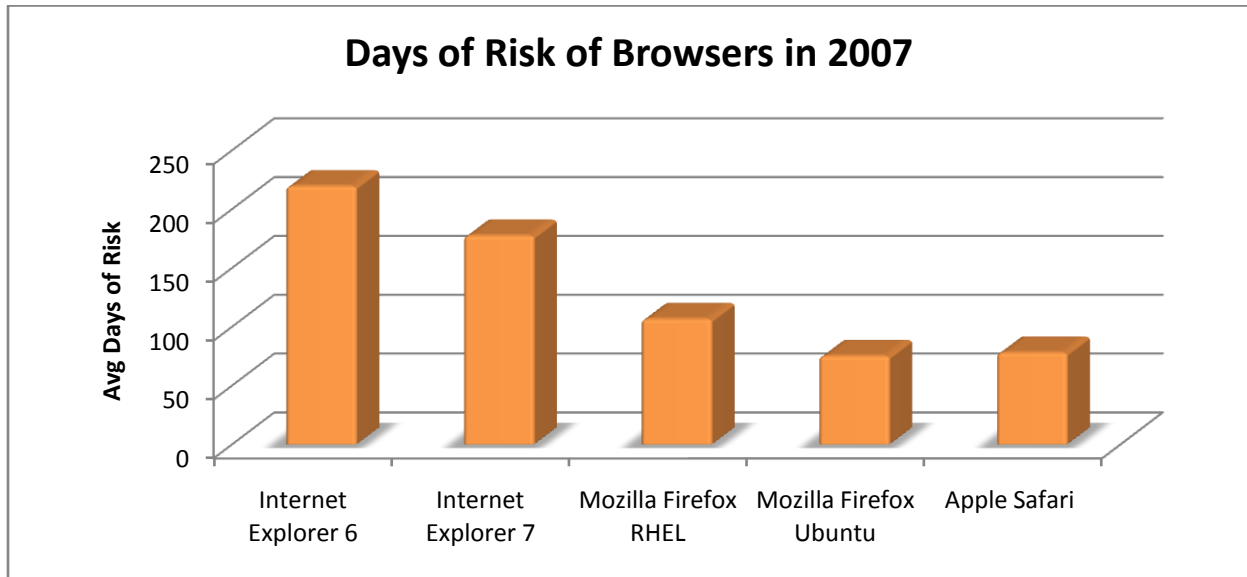
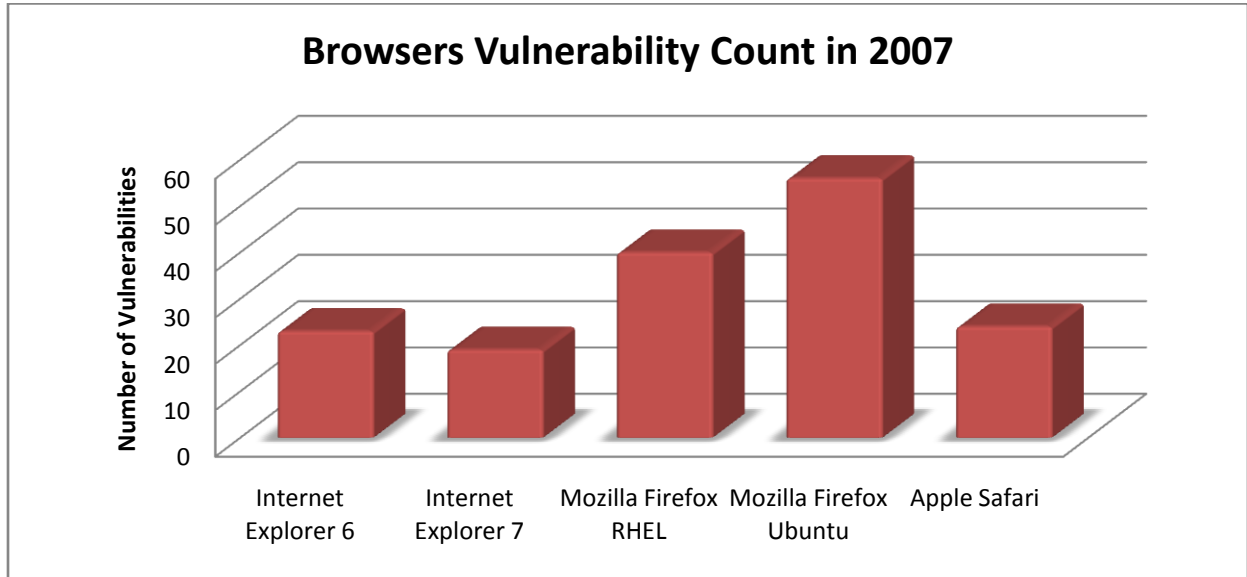
Following is the Web Browser Security Vulnerability data and days of Risk for the browsers for the year 2007. The browsers assessed were part of the Operating Systems assessed in this paper. They are Microsoft's **Internet Explorer 6 (Windows XP), Internet Explorer 7 (Windows Vista), Firefox 2.x (Red Hat), Firefox 2.x (Ubuntu) and Safari (Mac OS X 10.4)**

The data especially the average days of risk is highly accurate for Firefox (Red Hat and Ubuntu) and very close for Internet Explorer 6 & 7 (Windows XP, Windows Vista) where I was able to obtain initial disclosure dates for over 90% of the vulnerabilities. However, for Safari, I was able to get dates for only 6/24 (25%) vulnerabilities for Safari. So, the 78 days of risk could be low or could go higher. This again reflects the closed loop security mentality of Apple.

Coming back to the data, the best browser for year 2007 was Mozilla Firefox on the Ubuntu operating system, which although was exposed to 56 different vulnerabilities, had the lowest average days of risk at ~75.

---

<sup>4</sup> [http://security.itworld.com/5013/mac-hacked-first-in-contest-080327/page\\_1.html](http://security.itworld.com/5013/mac-hacked-first-in-contest-080327/page_1.html)



Browser	Number of Vulnerabilities	Average Days of Risk
Internet Explorer 6	23	219.53
Internet Explorer 7	19	177.46
Mozilla Firefox RHEL	40	106.6
Mozilla Firefox Ubuntu	56	75.15
Apple Safari	24	78

## FINAL OBSERVATIONS

So, does the high vulnerability count indicate that the Mac OS X is the most vulnerable of all the Operating Systems evaluated? Of course not... There are less than 200 known viruses targeting the Mac platform compared to the many hundreds for Windows. Again, if I was a malicious hacker, and motivated by financial incentives, I would want to write a virus that would **pawn** as many n00bs as possible on a dominant platform such as Windows. Owning as many boxes as possible would help a malicious hacker in launching a DDoS attacks or sending out spam or installing spyware on those machines where each click or install would pay the malicious hacker/spammer.

Recent reports are indicating the [increasing Mac market share](#) and this might tip it over an infection point which would bring more active attention from malware writers.

Adam J. O'Donnell, PhD, Director of Emerging Technologies at Cloudmark and has recently been using game theory to analyze at what point Macs become more targeted for malicious attack. He states,

**"Game theory shows that an inflection point will come when the rate at which a malware author can reliably compromise a PC rivals that of the Mac market share. It is at this time you will see monetized, profitable Mac malware start popping up."**

Derek Schatz<sup>5</sup> says it best when it may be possible to think about a relative security nirvana by patching your Operating System diligently, locking down the configuration and being careful with where you surf and what you trust on the Internet. For the average user, it is hard to make an OS secure but at the same time preserving usability, doesn't matter whether the Operating System is Windows or Linux or Mac OS. None is measurably better than the other and they only differ in how many security researchers/ malicious hackers are paying attention to it. Sure, there are some really secure Operating Systems such as OpenBSD or Trusted Solaris, but how many of your applications would run on them, those required for desktop usage.

So, Enterprises and regular users will continue to fight the never ending cycle of patching as new flaws continue to be found in their installed base of PC's. This is a battle that we lose a little more each month.

---

<sup>5</sup> <http://www.bloginfosec.com/2008/03/18/are-we-less-secure-now-than-before/>

## Appendix A

### Windows Vista – 2007

Date	Security Bulletin	Vulnerability	Vendor Severity	Component	Day Announced	Days of Risk
<b>4/3/2007</b>	MS07-017	CVE-2007-1212	Important	EMF	4/3/2007	
4/3/2007		CVE-2007-0038	Critical	Animated Cursor	12/20/2006	103
4/3/2007		CVE-2007-1215	Important	GDI		
<b>4/10/2007</b>	MS07-021	CVE-2006-6696	Critical	CSRSS	12/15/2006	115
4/10/2007		CVE-2007-1209	Important	CSRSS	1/19/2007	81
4/10/2007		CVE-2006-6797	Low	CSRSS	12/28/2006	102
<b>5/8/2007</b>	MS07-027	CVE-2007-0942	Important	Internet Explorer	5/8/2007	
5/8/2007		CVE-2007-0945	Critical	Internet Explorer		
5/8/2007		CVE-2007-0946	Important	Internet Explorer		
5/8/2007		CVE-2007-0947	Important	Internet Explorer	1/18/2007	110
5/8/2007		CVE-2007-2221	Critical	Internet Explorer		
<b>6/12/2007</b>	MS07-032	CVE-2007-2229	Moderate	ACL	6/12/2007	
6/12/2007	MS07-033	CVE -2007-1751	Critical	Internet Explorer	10/24/2006	228
6/12/2007		CVE -2007-1499	Moderate	Internet Explorer	3/15/2007	87
6/12/2007		CVE-2007-2222	Critical	Internet Explorer	10/24/2006	228
6/12/2007	MS07-034	CVE-2006-2111	Important	Windows Mail	12/15/2006	177
6/12/2007		CVE-2007-1658	Critical	Windows Mail	3/23/2007	79
6/12/2007		CVE-2007-2225	Important	Windows Mail		
6/12/2007		CVE-2007-2227	Moderate	Windows Mail		
<b>7/10/2007</b>	MS07-038	CVE-2007-3038	Moderate	Firewall	7/10/2007	
<b>8/14/2007</b>	MS07-042	CVE-2007-2223	Critical	XML Core Services	5/17/2006	447
8/14/2007	MS07-045	CVE-2007-2216	Important	Internet Explorer	5/8/2007	96
8/14/2007		CVE-2007-3041	Important	Internet Explorer		
8/14/2007	MS07-047	CVE-2007-3037	Important	Windows Media Player	3/19/2007	145
8/14/2007		CVE-2007-3035	Important	Windows Media Player	5/22/2007	82
8/14/2007	MS07-048	CVE-2007-3033	Important	Windows Gadgets	3/21/2007	143
8/14/2007		CVE-2007-3032	Moderate	Windows Gadgets	3/21/2007	143
8/14/2007		CVE-2007-3891	Moderate	Windows Gadgets		
8/14/2007	MS07-050	CVE-2007-1749	Critical	Internet Explorer	10/24/2006	290
<b>9/11/2007</b>	MS07-053	CVE-2007-3036	Important	UNIX	9/11/2007	
<b>10/9/2007</b>	MS07-056	CVE-2007-3897	Important	Windows Mail	7/11/2007	88
10/9/2007	MS07-057	CVE-2007-3892	Moderate	Internet Explorer	10/9/2007	
10/9/2007		CVE-2007-3893	Critical	Internet Explorer	4/1/2007	188
10/9/2007		CVE-2007-1091	Low	Internet Explorer	2/23/2007	226
10/9/2007		CVE-2007-3826	Low	Internet Explorer	7/13/2007	86

10/9/2007	MS07-058	CVE-2007-2228	Important	RPC	2/5/2007	244
<b>12/11/2007</b>	MS07-063	CVE-2007-5351	Important	SMB	12/11/2007	
12/11/2007	MS07-064	CVE-2007-3895	Critical	DirectX		
12/11/2007	MS07-066	CVE-2007-5350	Important	Windows Kernel		
12/11/2007	MS07-068	CVE-2007-0064	Critical	WMF		
12/11/2007	MS07-069	CVE-2007-3902	Critical	Internet Explorer	7/20/2007	141
12/11/2007		CVE-2007-3903	Critical	Internet Explorer	5/22/2007	199
12/11/2007		CVE-2007-5344	Critical	Internet Explorer	5/7/2007	214
12/11/2007		CVE-2007-5347	Critical	Internet Explorer	5/7/2007	214

163.69230

### Windows XP – 2007

Date	Security Bulletin	Vulnerabilities	Vendor Severity	Component	Day Announced	Days of Risk
<b>1/9/2007</b>	MS07-004	CVE-2007-0024	Critical	VML	10/3/2006	96
<b>2/13/2007</b>	MS07-005	CVE-2006-3448	Important	Interactive Training	5/15/2006	268
2/13/2007	MS07-006	CVE-2007-0211	Important	Windows Shell	2/13/2007	
2/13/2007	MS07-007	CVE-2007-0210	Important	Windows Image	2/13/2007	0
2/13/2007	MS07-008	CVE-2007-0214	Critical	ActiveX		
2/13/2007	MS07-009	CVE-2006-5559	Critical	ActiveX	10/27/2006	106
2/13/2007	MS07-011	CVE-2007-0026	Important	OLE		
2/13/2007	MS07-012	CVE-2007-0025	Important	MFC		
2/13/2007	MS07-013	CVE-2006-1311	Important	RichEdit		
2/13/2007	MS07-016	CVE-2006-4697	Critical	Internet Explorer		
2/13/2007		CVE-2007-0219	Critical	Internet Explorer		
2/13/2007		CVE-2007-0217	Critical	Internet Explorer	8/16/2006	177
<b>4/3/2007</b>	MS07-017	CVE-2006-5758	Important	GDI		
4/3/2007		CVE-2007-1211	Moderate	WMF		
4/3/2007		CVE-2007-1212	Important	EMF		
4/3/2007		CVE-2007-5586	Important	GDI		
4/3/2007		CVE-2007-0038	Critical	Animated Cursor	12/20/2006	103
4/3/2007		CVE-2007-1215	Important	GDI		
<b>4/10/2007</b>	MS07-019	CVE-2007-1204	Critical	UPnP	12/6/2006	
4/10/2007	MS07-020	CVE-2007-1205	Critical	MS Agent URL	12/11/2006	119
4/10/2007	MS07-021	CVE-2006-6696	Critical	CSRSS	12/15/2006	115
4/10/2007		CVE-2006-6797	Low	CSRSS	12/28/2006	102
4/10/2007	MS07-022	CVE-2007-1206	Important	Windows Kernel	12/12/2006	
<b>5/8/2007</b>	MS07-027	CVE-2007-0942	Critical	Internet Explorer		
5/8/2007		CVE-2007-0944	Critical	Internet Explorer	3/10/2006	418
5/8/2007		CVE-2007-0945	Critical	Internet Explorer		
5/8/2007		CVE-2007-2221	Critical	Internet Explorer		
<b>6/12/2007</b>	MS07-031	CVE-2007-2218	Critical	Windows Schannel	3/19/2007	

6/12/2007	MS07-033	CVE-2007-0218	Critical	Internet Explorer	10/24/2006	228
6/12/2007		CVE-2007-1750	Critical	Internet Explorer	10/24/2006	228
6/12/2007		CVE-2007-3027	Critical	Internet Explorer	10/24/2006	228
6/12/2007		CVE-2007-1751	Critical	Internet Explorer	10/24/2006	228
6/12/2007		CVE-2007-2222	Critical	Internet Explorer	10/24/2006	228
6/12/2007	MS07-034	CVE-2006-2111	Important	Windows Mail	12/15/2006	177
6/12/2007		CVE-2007-2225	Important	Windows Mail		
6/12/2007		CVE-2007-2227	Moderate	Windows Mail		
6/12/2007	MS07-035	CVE-2007-2219	Critical	Win32 API	4/11/2007	61
<b>8/14/2007</b>	MS07-042	CVE-2007-2223	Critical	XML Core	5/17/2006	
8/14/2007	MS07-043	CVE-2007-2224	Critical	OLE	10/3/2006	
8/14/2007	MS07-045	CVE-2007-2216	Critical	Internet Explorer	5/8/2007	
8/14/2007		CVE-2007-3041	Critical	Internet Explorer		
8/14/2007	MS07-046	CVE-2007-3034	Critical	GDI	3/27/2007	137
8/14/2007	MS07-047	CVE-2007-3037	Important	WMP	3/19/2007	145
8/14/2007		CVE-2007-3035	Important	WMP	5/22/2007	82
8/14/2007	MS07-050	CVE-2007-1749	Critical	Internet Explorer	10/24/2006	290
<b>9/11/2007</b>	MS07-053	CVE-2007-3036	Important	UNIX	9/11/2007	0
<b>10/9/2007</b>	MS07-055	CVE-2007-2217	Critical	Image Viewer		
10/9/2007	MS07-056	CVE-2007-3897	Critical	Windows Mail	7/11/2007	88
10/9/2007	MS07-057	CVE-2007-3892	Moderate	Internet Explorer	10/9/2007	0
10/9/2007		CVE-2007-3893	Critical	Internet Explorer	4/1/2007	188
10/9/2007		CVE-2007-1091	Low	Internet Explorer	2/23/2007	226
10/9/2007		CVE-2007-3826	Low	Internet Explorer	7/13/2007	86
10/9/2007	MS07-058	CVE-2007-2228	Important	RPC	2/5/2007	244
<b>11/13/2007</b>	MS07-061	CVE-2007-3896	Critical	Windows URI	7/26/2007	107
<b>12/11/2007</b>	MS07-064	CVE-2007-3895	Critical	DirectX		
12/11/2007	MS07-065	CVE-2007-3039	Important	Message Queuing	4/2/2007	249
12/11/2007	MS07-068	CVE-2007-0064	Critical	WMF		
12/11/2007	MS07-069	CVE-2007-3902	Critical	Internet Explorer	7/20/2007	141
12/11/2007		CVE-2007-3903	Critical	Internet Explorer	5/22/2007	199
12/11/2007		CVE-2007-5344	Critical	Internet Explorer	5/7/2007	214
12/11/2007		CVE-2007-5347	Critical	Internet Explorer	5/7/2007	214

161.52941

### RHEL4WS – Reduced Version Vulnerability list for 2007

Date	Security Bulletin	Vulnerability	Vendor Severity	Component	Day Announced	Days of Risk
<b>1/10/2007</b>						
7	RHSA – 2007: 0003	CVE – 2006 – 6101	Important	X.org	12/4/2006	36
1/10/2007		CVE – 2006 – 6102		X.org	12/4/2006	36
1/10/2007		CVE – 2006 – 6103		X.org	12/4/2006	36

<b>1/11/2007</b>	RHSA – 2007: 0011	CVE – 2006 – 4514	Moderate	GNOME	8/17/2006	144
<b>1/30/2007</b>	RHSA – 2007: 0014	CVE – 2006 – 4538	Moderate	Linux Kernel	9/18/2006	132
1/30/2007		CVE – 2006 – 4813	Important	Linux Kernel	12/14/2006	46
1/30/2007		CVE – 2006 – 4814	Moderate	Linux Kernel	12/20/2006	40
1/30/2007		CVE – 2006 – 5174	Important	Linux Kernel	10/6/2006	114
1/30/2007		CVE – 2006 – 5619	Important	Linux Kernel	11/1/2006	89
1/30/2007		CVE – 2006 – 5751	Important	Linux Kernel	12/7/2006	53
1/30/2007		CVE – 2006 – 5753	Moderate	Linux Kernel	1/30/2006	360
1/30/2007		CVE – 2006 – 5754	Important	Linux Kernel	12/29/2006	31
1/30/2007		CVE – 2006 – 5757	Low	Linux Kernel	11/6/2006	84
1/30/2007		CVE – 2006 – 5823	Low	Linux Kernel	11/8/2006	82
1/30/2007		CVE – 2006 – 6053	Low	Linux Kernel	11/23/2006	67
1/30/2007		CVE – 2006 – 6054	Low	Linux Kernel	11/23/2006	67
1/30/2007		CVE – 2006 – 6056	Low	Linux Kernel	11/23/2006	67
1/30/2007		CVE – 2006 – 6106	Moderate	Linux Kernel	12/18/2006	42
1/30/2007		CVE – 2006 – 6535	Moderate	Linux Kernel	10/25/2006	95
<b>2/6/2007</b>	RHSA – 2007: 0044	CVE – 2007 – 0494	Moderate	DNS - BIND	1/29/2007	7
<b>2/8/2007</b>	RHSA – 2007: 0008	CVE – 2006 – 6107	Moderate	D-BUS	12/14/2006	54
<b>2/15/2007</b>	RHSA – 2007: 0060	CVE – 2007 – 0452	Moderate	Samba	1/30/2007	15
<b>2/20/2007</b>	RHSA – 2007: 0086	CVE – 2007 – 1007	Critical	Gnome	2/19/2007	1
<b>2/23/2007</b>	RHSA – 2007: 0079	CVE – 2006 – 6077	Critical	Firefox	11/22/2006	91
2/23/2007		CVE – 2007 – 0008		Firefox	12/18/2006	65
2/23/2007		CVE – 2007 – 0009		Firefox	12/18/2006	65
2/23/2007		CVE – 2007 – 0775		Firefox		
2/23/2007		CVE – 2007 – 0777		Firefox		
2/23/2007		CVE – 2007 – 0778		Firefox	8/8/2006	195
2/23/2007		CVE – 2007 – 0779		Firefox	11/20/2006	93
2/23/2007		CVE – 2007 – 0780		Firefox		
2/23/2007		CVE – 2007 – 0800		Firefox		
2/23/2007		CVE – 2007 – 0981		Firefox	2/16/2007	7
2/23/2007		CVE – 2007 – 0994		Firefox		
2/23/2007		CVE – 2007 – 0995		Firefox		
2/23/2007		CVE – 2007 – 0996		Firefox	10/11/2006	132
2/23/2007		CVE – 2007 – 1092		Firefox	2/22/2007	1
<b>2/27/2007</b>	RHSA – 2007: 0085	CVE – 2007 – 0001	Important	Kernel	1/17/2007	40
2/27/2007		CVE – 2007 – 0006		Kernel	2/13/2007	14
<b>3/23/2007</b>	RHSA – 2007: 0124	CVE – 2007 – 1536	Moderate	File cmd	3/20/2007	3
<b>4/3/2007</b>	RHSA – 2007: 0126	CVE – 2007 – 1003	Important	X.org	2/8/2007	55

4/3/2007		CVE – 2007 – 1351		X.org	2/21/2007	42
4/3/2007		CVE – 2007 – 1352		X.org	2/21/2007	42
4/3/2007		CVE – 2007 – 1667		X.org	3/9/2007	24
4/3/2007	RHSA – 2007: 0095	CVE – 2007 – 0956	Critical	Kerberos	2/23/2007	40
4/3/2007		CVE - 2007 – 0957		Kerberos	2/8/2007	55
4/3/2007		CVE – 2007 – 1216		Kerberos	3/8/2007	25
<b>4/16/2007</b>						
<b>7</b>	RHSA – 2007: 0150	CVE – 2007 – 1351	Moderate	Freetype	2/21/2007	55
4/16/2007	RHSA – 2007: 0286	CVE – 2006 – 1057	Low	GNOME	4/7/2006	369
<b>5/1/2007</b>	RHSA – 2007: 0276	CVE – 2006 – 1174	Low	Shadow-utils	5/24/2006	337
5/1/2007	RHSA – 2007: 0252	CVE – 2006 – 7176	Low	Sendmail	10/26/2005	545
5/1/2007	RHSA – 2007: 0245	CVE – 2005 – 4268	Low	GNU cpio	11/10/2005	531
5/1/2007	RHSA – 2007: 0244	CVE – 2006 – 1058	Low	BusyBox	3/30/2006	391
5/1/2007	RHSA – 2007: 0235	CVE – 2006 – 7108	Low	Util-linux	1/9/2006	472
5/1/2007	RHSA – 2007: 0203	CVE – 2005 – 2475	Low	Unzip	8/2/2005	629
5/1/2007		CVE – 2005 – 4667		Unzip	1/25/2006	456
5/1/2007	RHSA – 2007: 0322	CVE – 2007 – 1859	Moderate	XScreenSaver	4/18/2007	13
<b>5/2/2007</b>	RHSA – 2007: 0354	CVE – 2007 – 2446	Critical	Samba	4/25/2007	7
<b>5/14/2007</b>						
<b>7</b>		CVE – 2007 – 2447		Samba	5/7/2007	7
5/14/2007	RHSA – 2007: 0065	CVE – 2006 – 6899	Moderate	BlueTooth	2/2/2007	102
5/14/2007	RHSA – 2007: 0353	CVE – 2007 – 1558	Moderate	Evolution	5/1/2007	13
<b>5/17/2007</b>						
<b>7</b>	RHSA – 2007: 0345	CVE – 2007 – 1856	Moderate	Cron	4/10/2007	37
5/17/2007	RHSA – 2007: 0343	CVE – 2007 – 2356	Moderate	GIMP	4/30/2007	17
<b>5/30/2007</b>						
<b>7</b>	RHSA – 2007: 0400	CVE – 2007 – 1362	Critical	Firefox	5/30/2007	0
5/30/2007		CVE – 2007 – 1562		Firefox	2/15/2007	105
5/30/2007		CVE – 2007 – 2867		Firefox		
5/30/2007		CVE – 2007 – 2868		Firefox		
5/30/2007		CVE – 2007 – 2869		Firefox	12/17/2006	163
5/30/2007		CVE – 2007 – 2870		Firefox	4/10/2007	50
5/30/2007		CVE – 2007 – 2871		Firefox	3/19/2007	71
5/30/2007	RHSA – 2007: 0391	CVE – 2007 – 2799	Moderate	File cmd	5/23/2007	7
5/30/2007	RHSA – 2007: 0389	CVE – 2007 – 1995	Moderate	Quagga	5/17/2007	13
<b>6/11/2007</b>						
<b>7</b>	RHSA – 2007: 0403	CVE – 2007 – 2754	Moderate	FreeType	5/15/2007	26
<b>6/13/2007</b>						
<b>7</b>	RHSA – 2007: 0494	CVE – 2007 – 2022	Important	Kdebase	6/10/2007	3
<b>6/14/2007</b>						
<b>7</b>	RHSA – 2007: 0501	CVE – 2006 – 4168	Moderate	Libexif	6/12/2007	2
<b>6/25/2007</b>						
<b>7</b>	RHSA – 2007: 0509	CVE – 2007 – 3257	Important	Evolution	6/14/2007	11
6/25/2007	RHSA – 2007: 0488	CVE – 2006 – 5158	Moderate	Linux Kernel	6/8/2007	17
6/25/2007		CVE – 2006 – 7203	Important	Linux Kernel	6/8/2007	17

6/25/2007		CVE – 2007 – 0773	Important	Linux Kernel	6/8/2007	17
6/25/2007		CVE – 2007 – 0958	Low	Linux Kernel	6/8/2007	17
6/25/2007		CVE – 2007 – 1353	Low	Linux Kernel	6/8/2007	17
6/25/2007		CVE – 2007 – 2172	Important	Linux Kernel	6/8/2007	17
6/25/2007		CVE – 2007 – 2525	Important	Linux Kernel	6/8/2007	17
6/25/2007		CVE – 2007 – 2876	Important	Linux Kernel	6/11/2007	14
6/25/2007		CVE – 2007 – 3104	Moderate	Linux Kernel	6/4/2007	21
<b>6/26/2007</b>						
<b>7</b>	RHSA – 2007: 0562	CVE – 2007 – 2442	Important	Kerberos	6/25/2007	1
6/26/2007		CVE – 2007 – 2443		Kerberos	6/25/2007	1
6/26/2007		CVE – 2007 – 2798		Kerberos	6/25/2007	1
<b>7/12/2007</b>						
<b>7</b>	RHSA – 2007 : 0675	CVE – 2007 – 3377	Moderate	Net::DNS	6/23/2007	19
7/12/2007	RHSA – 2007: 0519	CVE – 2007 – 3103	Moderate	X.Org	6/5/2007	37
<b>8/7/2007</b>	RHSA – 2007: 0765	CVE – 2007 – 0235	Moderate	Libgtop2	7/27/2007	10
<b>8/23/2007</b>						
<b>7</b>	RHSA – 2007: 0860	CVE – 2007 – 4131	Moderate	Tar	8/13/2007	10
<b>9/4/2007</b>	RHSA – 2007: 0873	CVE – 2007 – 4134	Moderate	Star	8/22/2007	12
9/4/2007	RHSA – 2007: 0795	CVE – 2006 – 1721	Moderate	Cyrus – SASL	4/24/2006	490
9/4/2007	RHSA – 2007: 0774	CVE – 2006 – 0558	Moderate	Linux Kernel	7/30/2007	34
9/4/2007		CVE – 2007 – 1217	Moderate	Linux Kernel	6/8/2007	86
<b>9/19/2007</b>						
<b>7</b>	RHSA – 2007: 0913	CVE – 2007 – 3999	Important	Nfs-utils	8/6/2007	43
9/19/2007	RHSA – 2007: 0898	CVE – 2007 – 4730	Moderate	X.org	9/11/2007	8
9/19/2007	RHSA – 2007: 0845	CVE – 2007 – 3106	Important	Ogg Vorbis	6/27/2007	82
9/19/2007		CVE – 2007 – 4029		Ogg Vorbis	6/5/2007	104
9/19/2007		CVE – 2007 – 4065		Ogg Vorbis	7/26/2007	53
9/19/2007		CVE – 2007 – 4066		Ogg Vorbis	7/25/2007	54
<b>9/26/2007</b>						
<b>7</b>	RHSA – 2007: 0513	CVE – 2006 – 4519	Moderate	GIMP	7/9/2007	77
9/26/2007		CVE – 2007 – 2949		GIMP	6/15/2007	101
9/26/2007		CVE – 2007 – 3741		GIMP	7/12/2007	74
<b>9/27/2007</b>						
<b>7</b>	RHSA – 2007: 0937	CVE – 2007 – 4573	Important	Linux Kernel	9/18/2007	9
<b>10/19/2007</b>						
<b>07</b>	RHSA – 2007: 0979	CVE – 2007 – 1095	Critical	Firefox	2/23/2007	236
10/19/2007		CVE – 2007 – 2292		Firefox	4/25/2007	174
10/19/2007		CVE – 2007 – 3511		Firefox	7/2/2007	107
10/19/2007		CVE – 2007 – 3844		Firefox	7/13/2007	96
10/19/2007		CVE – 2007 – 5334		Firefox	8/5/2007	74
10/19/2007		CVE – 2007 – 5337		Firefox	5/18/2007	151
10/19/2007		CVE – 2007 – 5338		Firefox	7/12/2007	97

10/19/2007		CVE – 2007 – 5339		Firefox		
10/19/2007		CVE – 2007 – 5340		Firefox		
<b>11/1/2007</b>	RHSA – 2007: 0939	CVE – 2006 – 6921	Moderate	Linux Kernel	9/24/2007	37
11/1/2007		CVE – 2007 – 2878	Important	Linux Kernel	7/10/2007	111
11/1/2007		CVE – 2007 – 3105	Low	Linux Kernel	7/16/2007	105
11/1/2007		CVE – 2007 – 3739	Moderate	Linux Kernel	9/18/2007	43
11/1/2007		CVE – 2007 – 3740	Important	Linux Kernel	9/4/2007	57
11/1/2007		CVE – 2007 – 3843	Low	Linux Kernel	9/4/2007	57
11/1/2007		CVE – 2007 – 3848	Important	Linux Kernel	8/6/2007	85
11/1/2007		CVE – 2007 – 4308	Moderate	Linux Kernel	8/15/2007	76
11/1/2007		CVE – 2007 – 4571	Moderate	Linux Kernel	9/13/2007	48
<b>11/15/2007</b>	RHSA – 2007: 1045	CVE – 2007 – 5846	Moderate	Net – SNMP	11/2/2007	13
11/15/2007	RHSA – 2007: 1016	CVE – 2007 – 4138	Critical	Samba	9/11/2007	64
11/15/2007		CVE – 2007 – 4572		Samba	9/18/2007	57
11/15/2007		CVE – 2007 – 5398		Samba	10/30/2007	15
11/15/2007	RHSA – 2007: 1003	CVE – 2007 – 3108	Moderate	OpenSSL	6/26/2007	139
11/15/2007		CVE – 2007 – 5135		OpenSSL	9/27/2007	48
11/15/2007	RHSA – 2007: 0969	CVE – 2007 – 5191	Moderate	Util – linux	10/5/2007	40
11/15/2007	RHSA – 2007: 0737	CVE – 2007 – 1716	Moderate	PAM	3/3/2007	252
11/15/2007		CVE – 2007 – 3102		PAM	7/11/2007	124
<b>11/26/2007</b>	RHSA – 2007: 1082	CVE – 2007 – 5947	Critical	Firefox	11/21/2007	5
11/26/2007		CVE – 2007 – 5959		Firefox	11/21/2007	5
11/26/2007		CVE – 2007 – 5960		Firefox	11/21/2007	5
<b>12/4/2007</b>	RHSA – 2007: 0740	CVE – 2007 – 2926	Moderate	ISC BIND	7/19/2007	135
12/4/2007	RHSA – 2007: 0724	CVE – 2007 – 3089	Critical	Firefox	5/19/2007	195
12/4/2007		CVE – 2007 – 3656		Firefox	7/8/2007	146
12/4/2007		CVE – 2007 – 3734		Firefox	7/17/2007	137
12/4/2007		CVE – 2007 – 3735		Firefox	7/17/2007	137
12/4/2007		CVE – 2007 – 3736		Firefox	5/11/2007	203
12/4/2007		CVE – 2007 – 3737		Firefox	6/5/2007	179
12/4/2007		CVE – 2007 – 3738		Firefox		
<b>12/10/2007</b>	RHSA – 2007: 1114	CVE – 2007 – 6015	Critical	Samba	11/23/2007	17
<b>12/12/2007</b>	RHSA – 2007: 1129	CVE – 2007 – 5964	Important	Autofs	12/4/2007	8

<b>12/19/2007</b>	RHSA – 2007: 1166	CVE – 2007 – 6352	Moderate	Libexif	12/14/2007	5
12/19/2007	RHSA – 2007: 1104	CVE – 2007 – 4997	Important	Linux Kernel	10/23/2007	56
12/19/2007		CVE – 2007 – 5494		Linux Kernel	10/2/2007	77
<b>12/20/2007</b>	RHSA – 2007: 1177	CVE – 2007 – 6285	Important	Autofs	12/19/2007	1
						<b>88.11594</b>

### Ubuntu 6.06 Vulnerabilities

Date	Security Bulletin	Vulnerabilities	Component	Day Announced	Days of Risk
1/3/2007	USN – 398 – 2	CVE – 2006 – 6497	Firefox	12/22/2006	11
1/3/2007		CVE – 2006 – 6498	Firefox		
1/3/2007		CVE – 2006 – 6499	Firefox	10/28/2006	65
1/3/2007		CVE – 2006 – 6501	Firefox	9/30/2006	93
1/3/2007		CVE – 2006 – 6502	Firefox	9/10/2006	113
1/3/2007		CVE – 2006 – 6503	Firefox	9/4/2006	119
1/3/2007		CVE – 2006 – 6504	Firefox	11/8/2006	55
1/4/2007	USN – 401 – 1	CVE – 2006 – 6107	D-Bus	12/14/2006	20
1/9/2007	USN – 403 – 1	CVE – 2006 – 6101	X.org	12/4/2006	35
1/9/2007		CVE – 2006 – 6102	X.org	12/4/2006	35
1/9/2007		CVE – 2006 – 6103	X.org	12/4/2006	35
1/15/2007	USN – 408 – 1	CVE – 2006 – 6143	Kerberos	1/10/2007	5
1/23/2007	USN – 411 – 1	CVE – 2006 – 5876	Libsoup2	1/15/2007	8
1/27/2007	USN – 398 – 4	CVE – 2006 – 6499	Firefox	12/19/2006	38
1/27/2007		CVE – 2006 – 6501	Firefox		
1/27/2007		CVE – 2006 – 6502	Firefox		
1/27/2007		CVE – 2006 – 6504	Firefox	11/8/2006	79
2/1/2007	USN – 415 – 1	CVE – 2007 – 0010	Gtk+ 2.0	1/25/2007	6
2/1/2007	USN – 416 – 1	CVE – 2006 – 4572	Linux Kernel	11/7/2006	84
2/1/2007		CVE – 2006 – 4814	Linux Kernel	12/20/2006	41
2/1/2007		CVE – 2006 – 5749	Linux Kernel	12/29/2006	32
2/1/2007		CVE – 2006 – 5753	Linux Kernel	1/30/2006	361
2/1/2007		CVE – 2006 – 5755	Linux Kernel	11/6/2006	85
2/1/2007		CVE – 2006 – 5757	Linux Kernel	11/6/2006	85
2/1/2007		CVE – 2006 – 5823	Linux Kernel	11/8/2006	83
2/1/2007		CVE – 2006 – 6053	Linux Kernel	11/23/2006	68
2/1/2007		CVE – 2006 – 6054	Linux Kernel	11/23/2006	68
2/1/2007		CVE – 2006 – 6056	Linux Kernel	11/23/2006	68
2/1/2007		CVE – 2006 – 6057	Linux Kernel	11/16/2006	75

2/1/2007		CVE – 2006 – 6106	Linux Kernel	12/18/2006	43
<b>2/5/2007</b>	USN – 418 – 1	CVE – 2007 – 0493	BIND	1/25/2007	10
2/5/2007		CVE – 2007 – 0494	BIND	1/29/2007	6
<b>2/6/2007</b>	USN – 419 – 1	CVE – 2007 – 0452	Samba	1/30/2007	6
2/6/2007		CVE – 2007 – 0454	Samba	1/8/2007	28
<b>2/22/2007</b>	USN – 425 – 1	CVE – 2007 – 0227	Slocate cmd	1/10/2007	42
<b>2/26/2007</b>	USN – 428 – 1	CVE – 2006 – 6077	Firefox	11/22/2006	94
2/26/2007		CVE – 2007 – 0008	Firefox	12/18/2006	68
2/26/2007		CVE – 2007 – 0009	Firefox	12/18/2006	68
2/26/2007		CVE – 2007 – 0775	Firefox		
2/26/2007		CVE – 2007 – 0776	Firefox	11/14/2006	102
2/26/2007		CVE – 2007 – 0777	Firefox		
2/26/2007		CVE – 2007 – 0778	Firefox	8/8/2006	198
2/26/2007		CVE – 2007 – 0779	Firefox	11/20/2006	96
2/26/2007		CVE – 2007 – 0780	Firefox		
2/26/2007		CVE – 2007 – 0800	Firefox		
2/26/2007		CVE – 2007 – 0981	Firefox	2/16/2007	10
2/26/2007		CVE – 2007 – 0995	Firefox		
2/26/2007		CVE – 2007 – 0996	Firefox	10/11/2006	135
2/26/2007		CVE – 2007 – 1092	Firefox	2/22/2007	4
<b>3/9/2007</b>	USN – 433 – 1	CVE – 2007 – 1246	Xine	3/3/2007	6
<b>3/12/2007</b>	USN – 435 – 1	CVE – 2007 – 1387	Xine	3/8/2007	4
<b>3/21/2007</b>	USN – 439 – 1	CVE – 2007 – 1536	LibMagic	3/20/2007	1
<b>3/27/2007</b>	USN – 443 – 1	CVE – 2007 – 1562	Firefox	2/15/2007	42
<b>4/3/2007</b>	USN – 448 – 1	CVE – 2007 – 1003	X.Org	2/8/2007	55
4/3/2007		CVE – 2007 – 1351	X.Org	2/21/2007	42
4/3/2007		CVE – 2007 – 1352	X.Org	2/21/2007	42
<b>4/4/2007</b>	USN – 449 – 1	CVE – 2007 – 0956	Kerberos	2/23/2007	41
4/4/2007		CVE – 2007 – 0957	Kerberos	2/8/2007	56
4/4/2007		CVE – 2007 – 1216	Kerberos	3/8/2007	26
<b>4/10/2007</b>	USN – 451 – 1	CVE – 2007 – 0006	Linux Kernel	2/13/2007	57
4/10/2007		CVE – 2007 – 0772	Linux Kernel	2/20/2007	50
4/10/2007		CVE – 2007 – 0958	Linux Kernel	3/9/2007	31
<b>4/18/2007</b>	USN – 453 – 1	CVE – 2007 – 1667	X.org	3/9/2007	39
<b>5/16/2007</b>	USN – 460 – 1	CVE – 2007 – 2444	Samba	3/20/2007	56
5/16/2007		CVE – 2007 – 2446	Samba	4/25/2007	21
5/16/2007		CVE – 2007 – 2447	Samba	5/7/2007	9
<b>5/17/2007</b>	USN – 461 – 1	CVE – 2007 – 1995	Quagga	5/17/2007	0
<b>5/23/2007</b>	USN – 464 – 1	CVE – 2007 – 1388	Linux Kernel		
5/23/2007		CVE – 2007 – 1496	Linux Kernel	3/13/2007	70
5/23/2007		CVE – 2007 – 1497	Linux Kernel	5/3/2007	20

5/23/2007		CVE – 2007 – 1592	Linux Kernel	5/3/2007	20
5/23/2007		CVE – 2007 – 1730	Linux Kernel	5/9/2007	14
5/23/2007		CVE – 2007 – 2172	Linux Kernel	5/8/2007	15
<b>5/30/2007</b>	USN – 466 – 1	CVE – 2007 – 2754	FreeType	5/15/2007	15
<b>6/1/2007</b>	USN – 468 – 1	CVE – 2007 – 1362	Firefox	5/30/2007	1
6/1/2007		CVE – 2007 – 2867	Firefox		
6/1/2007		CVE – 2007 – 2868	Firefox		
6/1/2007		CVE – 2007 – 2869	Firefox	12/17/2006	164
6/1/2007		CVE – 2007 – 2870	Firefox	4/10/2007	51
6/1/2007		CVE – 2007 – 2871	Firefox	3/19/2007	72
<b>6/11/2007</b>	USN – 439 – 2	CVE – 2007 – 2799	LibMagic	5/23/2007	18
6/11/2007	USN – 471 – 1	CVE – 2007 – 2645	Libexif	8/16/2006	295
<b>6/12/2007</b>	USN – 474 – 1	CVE – 2007 – 1859	Xscreensaver	4/18/2007	54
<b>6/26/2007</b>	USN – 477 – 1	CVE – 2007 – 2442	Kerberos	6/25/2007	1
6/26/2007		CVE – 2007 – 2443	Kerberos	6/25/2007	1
6/26/2007		CVE – 2007 – 2798	Kerberos	6/25/2007	1
6/26/2007	USN – 478 – 1	CVE – 2006 – 4168	Libexif	6/12/2007	14
<b>7/17/2007</b>	USN – 484 – 1	CVE – 2007 – 3564	Curl	6/27/2007	20
<b>7/19/2007</b>	USN – 489 – 1	CVE – 2006 – 4623	Linux Kernel	9/1/2006	318
7/19/2007		CVE – 2006 – 7203	Linux Kernel	5/17/2007	62
7/19/2007		CVE – 2007 – 0005	Linux Kernel	2/5/2007	164
7/19/2007		CVE – 2007 – 1000	Linux Kernel	3/14/2007	125
7/19/2007		CVE – 2007 – 1353	Linux Kernel	3/28/2007	111
7/19/2007		CVE – 2007 – 1861	Linux Kernel	5/4/2007	75
7/19/2007		CVE – 2007 – 2453	Linux Kernel	5/31/2007	49
7/19/2007		CVE – 2007 – 2525	Linux Kernel	5/31/2007	49
7/19/2007		CVE – 2007 – 2875	Linux Kernel	4/27/2007	82
7/19/2007		CVE – 2007 – 2876	Linux Kernel	6/11/2007	38
7/19/2007		CVE – 2007 – 2878	Linux Kernel	7/10/2007	9
7/19/2007		CVE – 2007 – 3380	Linux Kernel	6/27/2007	22
7/19/2007		CVE – 2007 – 3513	Linux Kernel	7/10/2007	9
7/19/2007	USN – 490 – 1	CVE – 2007 – 3089	Firefox		
7/19/2007		CVE – 2007 – 3285	Firefox	6/6/2007	43
7/19/2007		CVE – 2007 – 3656	Firefox	7/8/2007	11
7/19/2007		CVE – 2007 – 3734	Firefox	7/17/2007	2
7/19/2007		CVE – 2007 – 3735	Firefox	7/17/2007	2
7/19/2007		CVE – 2007 – 3736	Firefox	5/11/2007	68
7/19/2007		CVE – 2007 – 3737	Firefox	6/5/2007	44
7/19/2007		CVE – 2007 – 3738	Firefox		
<b>7/25/2007</b>	USN – 491 – 1	CVE – 2007 – 2926	Bind	7/19/2007	6
<b>7/31/2007</b>	USN – 493 – 1	CVE – 2007 – 3844	Firefox	7/13/2007	18

7/31/2007		CVE – 2007 – 3845	Firefox	7/21/2007	10
<b>8/16/2007</b>	USN – 498 – 1	CVE – 2007 – 3106	Vorbis	6/27/2007	49
8/16/2007		CVE – 2007 – 4029	Vorbis	6/5/2007	71
<b>8/20/2007</b>	USN – 500 – 1	CVE – 2007 – 4091	Rsync	8/16/2007	4
<b>8/28/2007</b>	USN – 504 – 1	CVE – 2007 – 2833	Emacs	1/29/2007	209
8/28/2007	USN – 506 – 1	CVE – 2007 – 4131	Tar	8/13/2007	15
<b>8/30/2007</b>	USN – 507 – 1	CVE – 2007 – 4601	TCP – libwrap	8/28/2007	2
<b>8/31/2007</b>	USN – 508 – 1	CVE – 2005 – 0504	Linux Kernel	1/25/2005	936
8/31/2007		CVE – 2007 – 2242	Linux Kernel	5/3/2007	118
8/31/2007		CVE – 2007 – 3104	Linux Kernel	6/4/2007	87
8/31/2007		CVE – 2007 – 3105	Linux Kernel	7/16/2007	45
8/31/2007		CVE – 2007 – 3848	Linux Kernel	8/6/2007	25
8/31/2007		CVE – 2007 – 4308	Linux Kernel	8/15/2007	16
<b>9/4/2007</b>	USN – 511 – 1	CVE – 2007 – 3999	Kerberos	8/6/2007	28
<b>9/7/2007</b>	USN – 511 – 2	CVE – 2007 – 4743	Kerberos	9/6/2007	1
<b>9/15/2007</b>	USN – 512 – 1	CVE – 2007 – 4826	Quagga		
9/15/2007	USN – 514 – 1	CVE – 2007 – 4730	X.org	9/11/2007	4
<b>9/20/2007</b>	USN – 516 – 1	CVE – 2007 – 2654	Xfsdump	5/30/2007	110
<b>9/24/2007</b>	USN – 517 – 1	CVE – 2007 – 4569	Kdm	9/12/2007	12
<b>9/25/2007</b>	USN – 518 – 1	CVE – 2007 – 3731	Linux Kernel	7/16/2007	69
9/25/2007		CVE – 2007 – 3739	Linux Kernel	9/18/2007	7
9/25/2007		CVE – 2007 – 3740	Linux Kernel	9/4/2007	21
9/25/2007		CVE – 2007 – 4573	Linux Kernel	9/18/2007	7
<b>9/29/2007</b>	USN – 522 – 1	CVE – 2007 – 3108	OpenSSL	6/26/2007	93
9/29/2007		CVE – 2007 – 5135	OpenSSL	9/27/2007	2
<b>10/4/2007</b>	USN – 525 – 1	CVE – 2007 – 4974	Libsndfile	9/19/2007	15
10/4/2007	USN – 526 – 1	CVE – 2007 – 3912	Debian	9/1/2007	33
<b>10/22/2007</b>	USN – 531 – 1	CVE – 2007 – 5365	DHCP	10/11/2007	11
10/22/2007	USN – 533 – 1	CVE – 2007 – 5191	Util-linux : Mount	10/5/2007	17
10/22/2007	USN – 534 – 1	CVE – 2007 – 4995	OpenSSL	10/6/2007	16
<b>10/23/2007</b>	USN – 535 – 1	CVE – 2006 – 2894	Firefox	2/11/2007	252
10/23/2007		CVE – 2007 – 1095	Firefox	2/23/2007	240
10/23/2007		CVE – 2007 – 2292	Firefox	4/25/2007	178
10/23/2007		CVE – 2007 – 3511	Firefox	7/2/2007	111
10/23/2007		CVE – 2007 – 5334	Firefox	8/5/2007	78
10/23/2007		CVE – 2007 – 5335	Firefox		
10/23/2007		CVE – 2007 – 5336	Firefox		
10/23/2007		CVE – 2007 – 5337	Firefox	5/18/2007	155
10/23/2007		CVE – 2007 – 5338	Firefox	7/12/2007	101
10/23/2007		CVE – 2007 – 5339	Firefox		
10/23/2007		CVE – 2007 – 5340	Firefox		

10/23/2007	USN – 531 – 2	CVE – 2007 – 5365	DHCP	10/11/2007	12
<b>11/16/2007</b>	USN – 544 – 1	CVE – 2007 – 4572	Samba	9/18/2007	58
11/16/2007		CVE – 2007 – 5398	Samba	10/30/2007	16
<b>11/26/2007</b>	USN – 546 – 1	CVE – 2007 – 5947	Firefox	11/21/2007	5
11/26/2007		CVE – 2007 – 5959	Firefox	11/21/2007	5
11/26/2007		CVE – 2007 – 5960	Firefox	11/21/2007	5
<b>12/8/2007</b>	USN – 555 – 1	CVE – 2007 – 5497	E2fsprogs	11/28/2007	10
<b>12/18/2007</b>	USN – 556 – 1	CVE – 2007 – 6015	Samba	11/23/2007	25
<b>12/19/2007</b>	USN – 558 – 1	CVE – 2006 – 6058	Linux Kernel	11/23/2006	386
12/19/2007		CVE – 2007 – 4133	Linux Kernel	8/22/2007	117
12/19/2007		CVE – 2007 – 4567	Linux Kernel		
12/19/2007		CVE – 2007 – 4849	Linux Kernel	9/27/2007	82
12/19/2007		CVE – 2007 – 4997	Linux Kernel	10/23/2007	56
12/19/2007		CVE – 2007 – 5093	Linux Kernel	9/2/2007	107
12/19/2007		CVE – 2007 – 5500	Linux Kernel	11/14/2007	35
12/19/2007		CVE – 2007 – 5501	Linux Kernel	11/16/2007	33
					<b>63.81208054</b>

### Apple OS X 10.4 Vulnerability List

Date	Security Bulletin	Vulnerabilities	Component	Day Announced	Days of Risk
<b>1/23/2007</b>	SU – 2007 – 001	CVE – 2007 – 0015	QuickTime	1/2/2007	21
<b>2/13/2007</b>	SU – 2007 – 002	CVE – 2007 – 0197	Finder	1/9/2007	
2/13/2007		CVE – 2007 – 0614	iChat	1/29/2007	14
2/13/2007		CVE – 2007 – 0710	iChat	1/29/2007	14
2/13/2007		CVE – 2007 – 0021	iChat	1/20/2007	23
2/13/2007		CVE – 2007 – 0023	UserNotification	1/22/2007	21
<b>3/5/2007</b>	QuickTime 7.1.5	CVE – 2007 – 0711	QuickTime		
3/5/2007		CVE – 2007 – 0712	QuickTime		
3/5/2007		CVE – 2007 – 0713	QuickTime		
3/5/2007		CVE – 2007 – 0714	QuickTime	8/14/2006	201
3/5/2007		CVE – 2007 – 0715	QuickTime		
3/5/2007		CVE – 2007 – 0716	QuickTime		
3/5/2007		CVE – 2007 – 0717	QuickTime		
3/5/2007		CVE – 2007 – 0718	QuickTime	12/6/2006	89
3/5/2007		CVE – 2006 – 4965	QuickTime		
3/5/2007		CVE – 2007 – 0059	QuickTime		
<b>3/13/2007</b>	SU – 2007 – 003	CVE – 2007 – 0719	ColorSync	1/6/2007	67
3/13/2007		CVE – 2007 – 0051	iPhoto	1/4/2007	69
3/13/2007		CVE – 2007 – 0467	Crash Reporter	1/28/2007	45

3/13/2007		CVE – 2007 – 0721	Disk Images		
3/13/2007		CVE – 2007 – 0722	Disk Images		
3/13/2007		CVE – 2006 – 6061	Disk Images	11/20/2006	113
3/13/2007		CVE – 2006 – 6062	Disk Images	11/20/2006	113
3/13/2007		CVE – 2006 – 5679	Disk Images	11/3/2006	130
3/13/2007		CVE – 2007 – 0229	Disk Images	1/10/2007	63
3/13/2007		CVE – 2007 – 0267	Disk Images	1/12/2007	61
3/13/2007		CVE – 2007 – 0299	Disk Images	1/11/2007	62
3/13/2007		CVE – 2007 – 0723	DS Plug-Ins		
3/13/2007		CVE – 2006 – 6097	GNU Tar	11/22/2006	111
3/13/2007		CVE – 2007 – 0318	HFS	1/13/2007	60
3/13/2007		CVE – 2007 – 0724	HID Family		
3/13/2007		CVE – 2007 – 1071	ImageIO	9/8/2006	185
3/13/2007		CVE – 2007 – 0733	ImageIO		
3/13/2007		CVE – 2006 – 5836	Kernel	11/9/2006	124
3/13/2007		CVE – 2006 – 6126	Kernel	11/23/2006	110
3/13/2007		CVE – 2006 – 6129	Kernel	11/26/2006	107
3/13/2007		CVE – 2006 – 6173	Kernel	11/28/2006	105
3/13/2007		CVE – 2007 – 0430	Kernel	1/19/2007	54
3/13/2007		CVE – 2006 – 6130	Networking	11/27/2006	
3/13/2007		CVE – 2007 – 0236	Networking	1/14/2007	59
3/13/2007		CVE – 2007 – 0728	Printing		
3/13/2007		CVE – 2007 – 0588	QuickDraw Manager	1/23/2007	50
3/13/2007		CVE – 2007 – 0463	Software Update	1/24/2007	49
3/13/2007		CVE – 2005 – 2959	Sudo		
3/13/2007		CVE – 2006 – 4829	WebLog	9/20/2006	
3/13/2007		CVE – 2007 – 0729	QuickTime	1/1/2007	72
<b>4/19/2007</b>	SU – 2007 – 004	CVE – 2007 – 0732	CarbonCore		
4/19/2007		CVE – 2006 – 5867	Fetchmail	1/4/2007	105
4/19/2007		CVE – 2006 – 0300	GNU Tar	2/16/2006	423
4/19/2007		CVE – 2007 – 0646	Help Viewer	1/30/2007	79
4/19/2007		CVE – 2007 – 0724	HID Family		
4/19/2007		CVE – 2007 – 0465	Installer	1/26/2007	83
4/19/2007		CVE – 2006 – 6143	Kerberos	1/10/2007	99
4/19/2007		CVE – 2007 – 0957	Kerberos	2/8/2007	71
4/19/2007		CVE – 2007 – 1216	Kerberos	3/8/2007	41
4/19/2007		CVE – 2007 – 0735	Libinfo		
4/19/2007		CVE – 2007 – 0736	Libinfo		
4/19/2007		CVE – 2007 – 0737	Login Window		
4/19/2007		CVE – 2007 – 0738	Login Window		
4/19/2007		CVE – 2007 – 0739	Login Window		

4/19/2007		CVE – 2007 – 0741	Network_cmds		
4/19/2007		CVE – 2007 – 0744	SMB		
4/19/2007		CVE – 2007 – 0022	System Configuration	1/21/2007	88
4/19/2007		CVE – 2007 – 0743	URL Mount		
4/19/2007		CVE – 2007 – 0747	WebDAV		
<b>5/1/2007</b>	QuickTime 7.1.6	CVE – 2007 – 2175	QuickTime	4/23/2007	8
<b>5/24/2007</b>	SU – 2007 – 005	CVE – 2007 – 0740	Alias Manager		
5/24/2007		CVE – 2007 – 0493	BIND	1/25/2007	
5/24/2007		CVE – 2007 – 0494	BIND	1/29/2007	115
5/24/2007		CVE – 2006 – 4095	BIND	9/5/2006	259
5/24/2007		CVE – 2006 – 4096	BIND	9/5/2006	259
5/24/2007		CVE – 2007 – 0750	CoreGraphics		
5/24/2007		CVE – 2007 – 0751	Crontabs		
5/24/2007		CVE – 2007 – 1558	Fetchmail	3/20/2007	64
5/24/2007		CVE – 2007 – 1536	File	3/21/2007	63
5/24/2007		CVE – 2007 – 2390	iChat		
5/24/2007		CVE – 2007 – 2386	mDNSResponder		
5/24/2007		CVE – 2007 – 0752	PPP	1/8/2007	136
5/24/2007		CVE – 2006 – 4573	Screen	10/25/2006	209
5/24/2007		CVE – 2005 – 3011	Texinfo	4/2/2007	52
<b>5/29/2007</b>	QuickTime 7.1.6	CVE – 2007 – 2388	QuickTime	5/7/2007	22
5/29/2007		CVE – 2007 – 2389	QuickTime		
<b>6/20/2007</b>	Mac OS X 10.4.10	CVE – 2007 – 2242	Networking		
<b>6/22/2007</b>	SU – 2007 – 006	CVE – 2007 – 2401	Safari	6/14/2007	8
6/22/2007		CVE – 2007 – 2399	Safari	6/14/2007	8
<b>7/11/2007</b>	QuickTime 7.2	CVE – 2007 – 2295	QuickTime	3/28/2006	463
7/11/2007		CVE – 2007 – 2392	QuickTime		
7/11/2007		CVE – 2007 – 2296	QuickTime	11/17/2006	234
7/11/2007		CVE – 2007 – 2394	QuickTime	4/2/2007	99
7/11/2007		CVE – 2007 – 2397	QuickTime	3/20/2007	111
7/11/2007		CVE – 2007 – 2393	QuickTime	3/22/2007	109
7/11/2007		CVE – 2007 – 2396	QuickTime	11/17/2006	234
7/11/2007		CVE – 2007 – 2402	QuickTime		
<b>7/31/2007</b>	SU – 2007 – 007	CVE – 2005 – 0758	Bzip2	4/22/2004	1179
7/31/2007		CVE – 2007 – 2403	CFNetwork		
7/31/2007		CVE – 2007 – 2404	CFNetwork		
7/31/2007		CVE – 2004 – 0996	Cscope	5/21/2003	1510
7/31/2007		CVE – 2004 – 2541	Cscope	11/11/2004	980
7/31/2007		CVE – 2005 – 0758	Gnuzip	4/22/2004	1179
7/31/2007		CVE – 2005 – 0758	iChat		
7/31/2007		CVE – 2007 – 2442	Kerberos	6/25/2007	36

7/31/2007		CVE – 2007 – 2443	Kerberos	6/25/2007	
7/31/2007		CVE – 2007 – 2798	Kerberos	6/25/2007	36
7/31/2007		CVE – 2007 – 3744	mDNSResponder	7/26/2007	5
7/31/2007		CVE – 2007 – 2406	Quartz Composer		
7/31/2007		CVE – 2007 – 2446	Samba	4/25/2007	96
7/31/2007		CVE – 2007 – 2447	Samba	5/7/2007	84
7/31/2007		CVE – 2007 – 2407	Samba		
7/31/2007		CVE – 2007 – 2408	Safari		
7/31/2007		CVE – 2007 – 0478	Safari	1/5/2007	206
7/31/2007		CVE – 2007 – 2409	Safari		
7/31/2007		CVE – 2007 – 2410	Safari		
7/31/2007		CVE – 2007 – 3742	Safari		
7/31/2007		CVE – 2007 – 3944	Safari		
11/5/2007	QuickTime 7.3	CVE – 2007 – 2395	QuickTime		
11/5/2007		CVE – 2007 – 3750	QuickTime	5/15/2007	170
11/5/2007		CVE – 2007 – 3751	QuickTime		
11/5/2007		CVE – 2007 – 4672	QuickTime	9/14/2007	51
11/5/2007		CVE – 2007 – 4676	QuickTime	9/14/2007	51
11/5/2007		CVE – 2007 – 4675	QuickTime	9/13/2007	52
11/5/2007		CVE – 2007 – 4677	QuickTime	9/14/2007	51
11/5/2007		CVE – 2007 – 4674	QuickTime	10/19/2007	16
11/14/2007	SU-2007-008	CVE – 2007 – 4678	AppleRAID		
11/14/2007		CVE – 2007 – 2926	BIND	7/19/2007	115
11/14/2007		CVE – 2005 – 0953	Bzip2	4/22/2005	922
11/14/2007		CVE – 2005 – 1260	Bzip2	5/12/2005	902
11/14/2007		CVE – 2007 – 4679	CFFTP		
11/14/2007		CVE – 2007 – 4680	CFNetwork	5/15/2007	179
11/14/2007		CVE – 2007 – 0464	CFNetwork	1/25/2007	289
11/14/2007		CVE – 2007 – 4681	CoreFoundation		
11/14/2007		CVE – 2007 – 4682	CoreText		
11/14/2007		CVE – 2007 – 3999	Kerberos	8/6/2007	98
11/14/2007		CVE – 2007 – 4743	Kerberos	9/6/2007	68
11/14/2007		CVE – 2007 – 3749	Kernel	9/7/2007	67
11/14/2007		CVE – 2007 – 4683	Kernel		
11/14/2007		CVE – 2007 – 4684	Kernel		
11/14/2007		CVE – 2007 – 4685	Kernel	9/14/2007	60
11/14/2007		CVE – 2006 – 6127	Kernel	9/14/2007	60
11/14/2007		CVE – 2007 – 4686	Kernel	3/19/2007	235
11/14/2007		CVE – 2007 – 4687	Remote_cmds	9/14/2007	60
11/14/2007		CVE – 2007 – 4688	Networking		
11/14/2007		CVE – 2007 – 4269	Networking	9/8/2007	66

11/14/2007		CVE – 2007 – 4689	Networking		
11/14/2007		CVE – 2007 – 4267	Networking	7/16/2007	118
11/14/2007		CVE – 2007 – 4268	Networking	8/8/2007	96
11/14/2007		CVE – 2007 – 4690	NFS		
11/14/2007		CVE – 2007 – 4691	NSURL		
11/14/2007		CVE – 2007 – 0646	Safari	1/30/2007	
11/14/2007		CVE – 2007 – 4692	Safari		
11/14/2007		CVE – 2007 – 4693	SecurityAgent		
11/14/2007		CVE – 2007 – 4694	Safari		
11/14/2007		CVE – 2007 – 4695	Safari		
11/14/2007		CVE – 2007 – 4696	Safari		
11/14/2007		CVE – 2007 – 4697	Safari		
11/14/2007		CVE – 2007 – 4698	Safari		
11/14/2007		CVE – 2007 – 3758	Safari	9/28/2007	46
11/14/2007		CVE – 2007 – 3760	Safari	9/27/2007	47
11/14/2007		CVE – 2007 – 4671	Safari	6/11/2007	153
11/14/2007		CVE – 2007 – 4699	Safari		
11/14/2007		CVE – 2007 – 4700	Safari		
11/14/2007		CVE – 2007 – 4701	Safari		
12/13/2007	QuickTime 7.3.1	CVE – 2007 – 6166	QuickTime	9/20/2006	443
12/13/2007		CVE – 2007 – 4706	QuickTime	8/29/2007	104
12/13/2007		CVE – 2007 – 4707	QuickTime		
12/17/2007	SU – 2007 – 009	CVE – 2007 – 4708	Address Book		
12/17/2007		CVE – 2007 – 4710	ColorSync		
12/17/2007		CVE – 2007 – 5847	Core Foundation		
12/17/2007		CVE – 2007 – 5850	Desktop Services		
12/17/2007		CVE – 2007 – 4131	GNU Tar	8/13/2007	124
12/17/2007		CVE – 2007 – 5851	iChat		
12/17/2007		CVE – 2007 – 5853	IO Storage Family		
12/17/2007		CVE – 2007 – 5854	Launch Services		
12/17/2007		CVE – 2007 – 5855	Mail		
12/17/2007		CVE – 2007 – 5858	Safari		
12/17/2007		CVE – 2007 – 5859	Safari		
12/17/2007		CVE – 2007 – 4572	Samba	9/18/2007	89
12/17/2007		CVE – 2007 – 3876	SMB	7/16/2007	151
12/17/2007		CVE – 2007 – 5861	Spotlight		
12/17/2007		CVE – 2007 – 1218	Tcpdump	3/14/2007	273
12/17/2007		CVE – 2007 – 3798	Tcpdump	7/31/2007	137
12/17/2007		CVE – 2007 – 5858	Safari		

170.92631

## **Appendix B**

### Frequently Asked Questions

#### **Q1. Is this supposed to be a critical review of Jeff Jones Vulnerability Report?**

Yes: If you noticed in Jeff's report, his Windows XP and Windows Vista update histogram charts, the Y-Axis was up to 50 which on a first glance might indicate a low number of updates for that week. He is not consistent across. Check out his charts on RedHat and OS X in his 1 year vulnerability report to see what I mean.

No: I will say it would be a more in depth and accurate representation of what matters most NOW and not simply looking at how much Windows Vista has progressed in terms of incorporating security as part of the Operating System development and not an afterthought.

#### **Q2. Why did you include QuickTime and some other core applications as part of this assessment?**

In the present day security risk landscape, the network is no longer the primary threat for attacks. In enterprises, most firewalls block 99% of ports with 80,25 and 443 being some of the exceptions. So we are now secure right? Wrong. Today's malicious hackers are exploiting the application layer more than ever. Inject code, own the application that's running, control memory and with it the hardware, you now Own the box.

Applications such as QuickTime have been tightly integrated in the Macintosh OS X. Excluding QuickTime would mean I am removing a significant component of the Mac OS X Security assessment.

#### **Q3. How can you compare Linux distros with Windows – how did you do this apples to apples comparison?**

I used a role based approach and tried to level the playing field by having the same set of components across the different Operating Systems which were compared in this report. If you look, under each section, I excluded/included certain components leveling the playing field throughout.

#### **Q4. How do I know the numbers and analysis you presented are accurate?**

Unlike Jeff's report where we only get to see vulnerability information relating to Windows XP and Windows Vista, I have included the vulnerability information used for all the Operating Systems. Is this report 100% accurate? I doubt it especially in the case of Apple (OS X, QuickTime, Safari) where vulnerability information was severely limited/not available which is rather unfortunate because we don't get to see a comparison of the different operating systems especially because Apple likes to tout the security<sup>6</sup> of its Operating System

---

6

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=spam\\_\\_malware\\_and\\_vulnerabilities&articleId=9069538&taxonomyId=85](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=spam__malware_and_vulnerabilities&articleId=9069538&taxonomyId=85)

## Appendix C

### SOURCES

The analysis in this report uses vulnerability and security information compiled and cross checked using several sources of data on the Internet.

**Microsoft TechNet:** <http://www.microsoft.com/technet/security/current.aspx>

**RedHat Security:** <https://rhn.redhat.com/errata/rhel4ws-errata-security.html>

**Ubuntu Security:** <http://www.ubuntu.com/usn>

**Apple Security:** <http://docs.info.apple.com/article.html?artnum=305391>

**Firefox:** <http://www.mozilla.org/projects/security/known-vulnerabilities.html#Firefox>

#### Other Security Sites & Resources:

<http://www.trapkit.de/advisories>

<http://www.zerodayinitiative.com/advisories/>

<http://www.securiteam.com/cves/2006/>

<http://securityreason.com/>

<http://labs.iddefense.com/intelligence/vulnerabilities/?intYear=2007>

<http://www.securityfocus.com/bid>

<http://research.eeye.com/html/advisories/published/index.html>

[http://secunia.com/secunia\\_research/](http://secunia.com/secunia_research/)

<https://webapp.iss.net/Search.do?keyword=CVE-2007-3826&searchType=keywd&x=13&y=8>