



# WINDOWS VISTA

## 90 DAY VULNERABILITY REPORT

By Jeffrey R. Jones

Security Guy



## Contents

Executive Summary .....	2
The Security Researcher Ecosystem .....	3
Windows Vista - The First 90 Days .....	3
Vulnerability Fixes.....	3
Vulnerability Disclosures.....	3
Other Modern Operating Systems .....	4
Windows XP.....	4
Red Hat Enterprise Linux 4 Workstation ..	5
RHEL4WS – Reduced Component Set .....	5
Ubuntu 6.06 LTS .....	6
Novell SUSE Linux Enterprise Desktop 10	6
Apple Mac OS X v10.4 .....	7
The Comparison – Putting it All Together ....	7

## EXECUTIVE SUMMARY

February 28<sup>th</sup> marked 90 days that Windows Vista had been available to business customers. December brought the first public disclosure of a vulnerability and February brought the first Security Bulletin affecting Windows Vista. Has it been a good or a bad 90 days for security vulnerabilities?

This brief paper analyzes the vulnerability disclosures and fixes for Windows Vista and looks at it in the context of its predecessor, Windows XP, along with several other modern workstation operating systems including Red Hat, Ubuntu, Novell and Apple products.

The results of the analysis show that Windows Vista has an improved security vulnerability profile over its predecessor and a significantly better profile relative to comparable modern competitive operating systems.



## THE SECURITY RESEARCHER ECOSYSTEM

Before jumping into the 90-day analysis, let's look a bit at the ecosystem of security researchers and the science of finding security flaws in software. According to the [IBM Internet Security Systems X-Force 2006 Trend Statistics](#), total new software vulnerabilities have grown from 1918 in 2001 to 7247 in 2006, an increase of roughly 278% in annual vulnerability disclosures.

This is one of many indications that the security researcher industry is maturing, growing and becoming more proficient at finding and disclosing software vulnerabilities. In recent years, tools have improved significantly, several professional code scanning tools have released as products and newer techniques such as Fuzz testing have been developed to further stress the boundaries of software security.

How much more scrutiny does a new operating system face today compared with the year 2001? I can't easily put a number on it, but in my opinion, it does seem like there are more researchers, better trained, and with better tools and techniques than ever before – creating an ecosystem better able to find and disclose security vulnerabilities.

## WINDOWS VISTA - THE FIRST 90 DAYS

Windows Vista, the successor to Windows XP, released to business users on November 30, 2006. Since the release of Windows XP, the Microsoft approach to security has gone through some significant changes. In January 2002, only a few months after the release of Windows XP, Microsoft launched their Trustworthy Computing initiative and began to revise their entire product development process with the goal of long-term, ongoing, security improvement for customers.

How much impact has that commitment had for Windows Vista security?

It is too soon to get a complete picture, but as of February 28, 2007, the full release of Windows Vista has been in production use by business customers for 90 days – the minimum period for which I think we can start to look for indications of improvement.

To get a complete view of the early vulnerability indicators, we will look at vulnerability fixes and vulnerability disclosures in the first 90 days.

### VULNERABILITY FIXES

Microsoft released Security Bulletin MS07-010 on February 13, 2007 to address a vulnerability (CVE-2006-5270) in the Microsoft Malware Engine, a shipping component of Windows Vista. Microsoft rated this vulnerability as Critical and it had a corresponding High severity rating assigned by the National Institute of Standards (NIST) in the [National Vulnerability Database](#) (NVD). This was the only vulnerability fixed affecting Windows Vista in the first 90 days.

### VULNERABILITY DISCLOSURES



In addition to the vulnerability fixed in February, there were four additional vulnerability disclosures during Windows Vista's first 90 days<sup>1</sup>. I will outline some basic information on these:

Vulnerability Identifier	Brief Description	NVD Rating
CVE-2006-6696	CSRSS/MessageBox double-free	High
CVE-2007-0612	IE denial-of-service (Web site can crash IE)	Low
CVE-2007-0675	Speech recognition attack via sound object	Medium <sup>2</sup>
CVE-2007-0843	Bypass permissions to determine file attributes	Medium

I will also note that all four of these were disclosed after the product shipped to business customers and there are not currently any vulnerabilities that had been disclosed prior to ship that went unfixed.

So, in summary, 5 total vulnerability disclosures in the first 90 days, with one of them fixed and one High severity one pending, along with 2 Mediums and a Low severity vulnerability. Is that good, bad or indifferent? Let's look at other operating systems and see if they can provide some context for these numbers.

## OTHER MODERN OPERATING SYSTEMS

In this section, I will look at the first 90 days of availability for Windows XP, Red Hat Enterprise Linux 4 WS, Ubuntu 6.06 LTS, Novell SUSE Linux Enterprise Desktop 10 and Mac OS X 10.4 (Tiger).

### WINDOWS XP

First, let's start with a comparison to the first 90 days of Windows XP, which shipped on October 25, 2001.

- When Windows XP shipped, there were already three vulnerabilities in Internet Explorer (IE) which had been disclosed and fixed 3 weeks prior. Consequently, new users needed to apply an IE patch immediately to address those.
- Microsoft fixed a total (including the 3 mentioned above) of 14 vulnerabilities in the first 90 days the product was available. 8 of the vulnerabilities were rated High severity in the NVD.
- At the end of the 90 day period, a total of 4 publicly disclosed vulnerabilities did not yet have a patch available from Microsoft.

<sup>1</sup> Disclosures are harder to track than fixes, since for fixes one only has to check the vendor site, but for disclosures one has to check many locations where vulnerability information could have been published and then validate that the vulnerability applies. This is as accurate as I can be, but if someone identifies further vulnerability disclosures that I missed, I will acknowledge it and update appropriately.

<sup>2</sup> Microsoft has disputed the severity of this issue, since a victim would need to visit a malicious site and then either leave the machine immediately or do nothing (and be very quiet) while hearing a long, set of sequential verbal commands attempting to do something on the machine.

March 21, 2007

So, with respect to its predecessor product, Windows Vista seems to have a better initial 90 days. Next, look at some of the more modern Linux Workstation products to see how they've done in their early days.

## RED HAT ENTERPRISE LINUX 4 WORKSTATION

Red Hat is the most popular Enterprise Linux distribution, so their latest supported release, Red Hat Enterprise Linux 4 Workstation (rhel4ws), will be the first I examine<sup>3</sup>.

- When rhel4ws shipped on February 15, 2005, there were 129 vulnerabilities already publicly disclosed in shipping components prior to general availability – 40 of them High severity. On ship day, Red Hat issued 27 security advisories to address 64 of them and fixed a further 35 within the first 90 days.
- During the first 90 days, Red Hat fixed a total of 181 vulnerabilities in rhel4ws. 58 of those fixed were rated High severity in the NVD.
- At the end of the 90 day period, a total of 85 publicly disclosed vulnerabilities did not yet have a patch from Red Hat – 30 from before the product shipped and another 55 disclosed during the period.

Of course, I can already hear the objections about how “unfair” it is for me to “count” the vulnerabilities for all of the components for the product that Red Hat ships and supports as Red Hat Enterprise Linux 4 WS.

## RHEL4WS – REDUCED COMPONENT SET

Red Hat and other Linux distribution vendors add value to their workstation distributions by including and supporting many applications that don't have a comparable component on a Microsoft Windows operating system. It is a common objection to any Windows and Linux comparison that counting the “optional” applications against the Linux distribution is unfair, so I've completed an extra level of analysis to exclude component vulnerabilities that do not have comparable functionality shipping with a Windows OS. You may read [Red Hat and Windows - Defining an Apples-to-Apples Workstation Build](#) for more details, but basically I install a rhel4ws computer and:

- I exclude any component that is not installed by default, which includes all optional “server” components that ship with rhel4ws.
- I additionally exclude the *Thunderbird* (rich email), *text-internet*, *graphics* (the gimp stuff) and *office* (OpenOffice) installation groups.
- I use the rpm command to list out all packages that get installed and use that package list to filter vulnerabilities.

Basically, this 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

---

<sup>3</sup> The source for this information is <http://rhn.redhat.com/errata>. Disclosure dates are compile from many sites, including (but not limited to) <http://nvd.nist.gov> and other vendor web sites.

OpenOffice and other optional stuff that a Windows system wouldn't have by default. This reduced rhel4ws build is then examined for comparison:

- The reduced rhel4ws set of components had 86 vulnerabilities already publicly disclosed prior to general availability. Patches available on the first day of ship addressed 34 of these.
- During the first 90 days, Red Hat fixed 137 vulnerabilities affecting the reduced rhel4ws set of components. 40 of those addressed were High severity.
- At the end of the 90 day period, a total of 64 publicly disclosed vulnerabilities in the reduced set of components did not yet have a patch from Red Hat.

So, though the reduced component set of rhel4ws did have a better 90 day period than the full product, Red Hat customers did face a reasonably large number of vulnerabilities in the first 90 days.

## UBUNTU 6.06 LTS

Next up for comparison is Ubuntu 6.06 LTS. Ubuntu is considered by many to be the most popular up and coming Linux distribution and they committed to long-term support (LTS) for the Ubuntu 6.06 version released on June 1, 2006. Long-term support is a key requirement for a distribution to be considered for use within most businesses, so this makes the support commitment a strategic one for Ubuntu.

- Ubuntu 6.06 LTS had 24 vulnerabilities already publicly disclosed prior to the June 1, 2006 availability date. Seven of the 9 High severity issues were fixed one week later on June 8.
- During the first 90 days, Ubuntu fixed 71 vulnerabilities affecting Ubuntu 6.06 LTS. 27 of those fixed were rated High severity in the NVD.
- At the end of the 90 day period, there were at least<sup>4</sup> 29 publicly disclosed vulnerabilities in Ubuntu 6.06 LTS did not yet have a patch from Ubuntu.

Ubuntu customers seem to have had a better first 90 days than Red Hat customers, and in fact had the lowest vulnerabilities counts of any of the Linux distributions I examined. Given that Ubuntu 6.06 shipped 16 months after rhel4ws, it may be that they benefitted from the open source contributions of Red Hat.

## NOVELL SUSE LINUX ENTERPRISE DESKTOP 10

The final and most recent Linux-based workstation product that I will examine is Novell's SUSE Linux Enterprise Desktop 10 (SLED10), which released on July 17, 2006.

- Novell SLED10 had 19 vulnerabilities already publicly disclosed prior to the ship date and Novell provided fixes for 13 of these in the first 90 days. Five of the vulnerabilities were High severity.

---

<sup>4</sup> For "disclosed, but unpatched" numbers on the Linux distributions I am only counting ones that the vendor validates by later issuing a patch. This means that for a product like rhel4ws, the number is pretty accurate. However, for newer releases, it means that the numbers is a minimum and is likely to rise over time.



- During the first 90 days, Novell fixed a total of 80 vulnerabilities affecting SLED10, of which 30 were rated High severity in the NVD.
- At the end of the 90 day period, there were at least<sup>4</sup> 31 publicly disclosed vulnerabilities in SLED10 that did not yet have a patch from Novell.

## APPLE MAC OS X V10.4

Apple advertising conveys the message that Mac OS X does not have the same security issues that face other operating systems, but upon examining the first 90 days of their most recent release Tiger (v10.4), here is what I found.

- Mac OS X v10.4 had 10 vulnerabilities already publicly disclosed prior to the April 29, 2005 ship date and Apple provided fixes for 4 of these during the first 90 days after ship. Four of the vulnerabilities were High severity.
- During the first 90 days, Apple fixed a total of 20 vulnerabilities affecting Mac OS X v10.4, of which 8 were rated High severity in the NVD.
- At the end of the 90 day period, there Mac OS X v10.4 still had 17 publicly disclosed vulnerabilities that did not yet have a patch from Apple.

The just data doesn't support their marketing.

## THE COMPARISON – PUTTING IT ALL TOGETHER

Having analyzed the vulnerability situation for the previous Windows workstation product, Windows XP, and several Linux distributions and Mac OS X (Tiger), we now have a broad set of informational context in which to view the first 90 days of Windows Vista.

Figure 1 shows the set of products examined graphically, stacking the fixed and the publicly disclosed, but unfixed, vulnerabilities for the first 90 days of availability for each operating system.

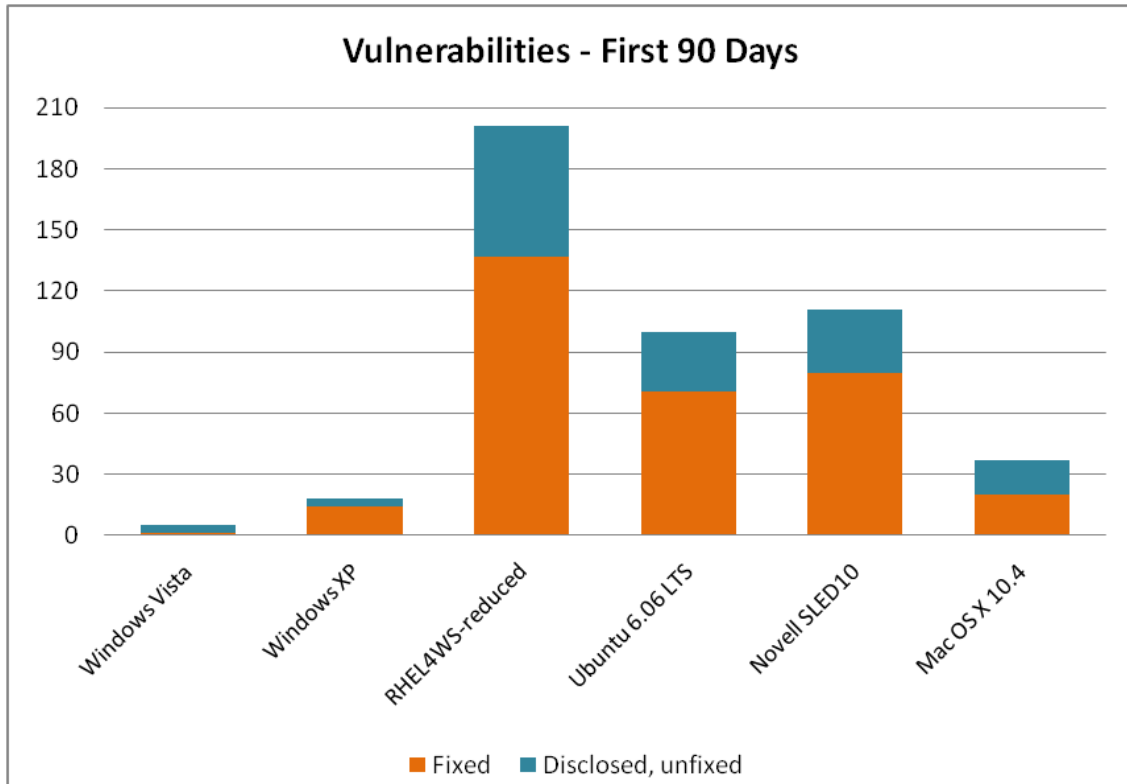


Figure 1: Operating System Vulnerabilities - First 90 days of general availability

As can be seen, Windows Vista shows an improved situation over its predecessor as well as modern Enterprise Linux distributions and the most recent major Mac OS X release.

As an early and tentative indicator, this is good news for Windows Vista security, but keep in mind that it is early days yet, and we should have a more informative view after we pass the 6-month and 1-year milestones.



## ABOUT THE AUTHOR

Jeff Jones is a Security Strategy Director in Microsoft's Trustworthy Computing group. In this role, Jeff draws upon his security experience to work with enterprise CSOs and Microsoft's internal security teams to drive practical and measurable security improvements into Microsoft process and products. Prior to his strategic position at Microsoft, Jeff was the vice president of product management for security products at Network Associates where his responsibilities included PGP, Gauntlet and Cybercop products, and several improvements in the McAfee product line. These latest positions cap a 20 year hands on career in security, performing risk assessments, building custom firewalls and being involved in DARPA security research projects while part of Trusted Information Systems. Jeff is a frequent global speaker and writer on security topics ranging from the very technical to more high level, CxO-focused topics such as Security TCO and metrics.

Jeff actively encourages readers to challenge his assumptions, analysis and conclusions and provide critical feedback – but asks for equal (or better) rigor in methodology and analysis to support the challenges, as opposed to enthusiastic espousal of unsupported evangelistic fervor.