

Microsoft Vista vs Windows XP SP2 Vulnerability Report 2007

<http://blogs.technet.com/security>

http://blogs.csoonline.com/blog/jeff_jones



by

Jeffrey R. Jones
Security Guy

(and Microsoft Director)

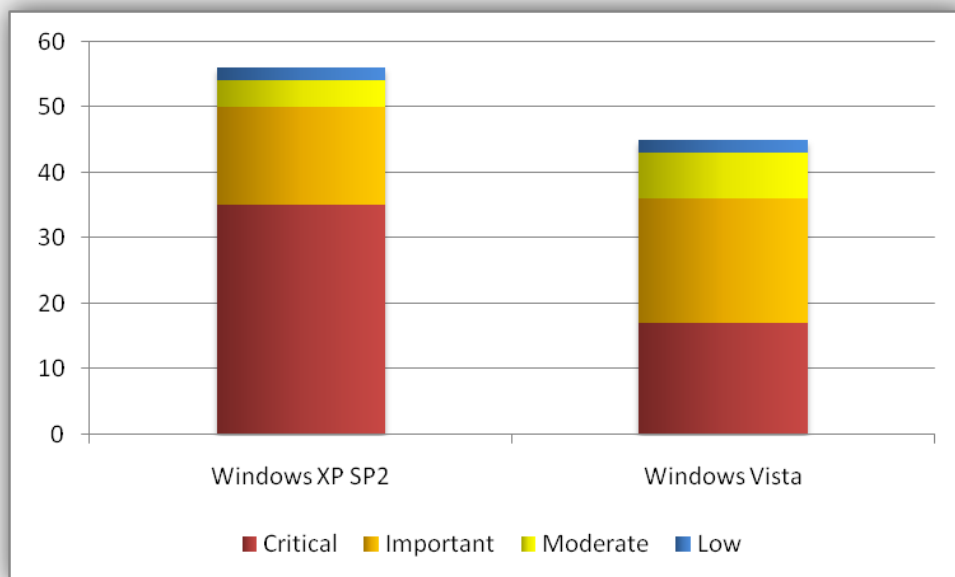
*Windows Vista users
experienced fewer high
severity vulnerabilities than
Windows XP SP2 users
during 2007.*

In the wake of my [Windows Vista One Year Vulnerability Report](#), I have received many questions regarding the current vulnerability record of Windows Vista as compares with Windows XP SP2.

This short paper is a compilation of vulnerability data for Microsoft Windows Vista and Microsoft Windows XP SP2 for calendar year 2007 and a brief analysis to see if any benefit is apparent for users of one OS over the other.

I found that Windows Vista offers benefit over Windows XP SP2 in the following ways for 2007:

- Windows Vista had 30% fewer Security Bulletins than Windows XP
- Windows Vista had 20% fewer vulnerabilities than Windows XP
- Windows Vista had 28% fewer Critical and Important vulnerabilities than Windows XP
- 26 vulnerabilities on Windows Vista are less severe for any users running as standard user.



About the Author.....	3
Introduction	4
Windows Vista	5
Windows XP SP2.....	6
Summary	7
Appendix A: Interpreting the Data.....	9
Appendix B: Data Sources	10

About the Author

Jeff Jones is a Security Strategy Director in Microsoft's Trustworthy Computing group. In this role, Jeff draws upon his years of 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.

Introduction

In my [Windows Vista One Year Vulnerability Report](#), I found that the first year of Windows Vista had an improved security vulnerability profile over its predecessor, Windows XP, in its first year.

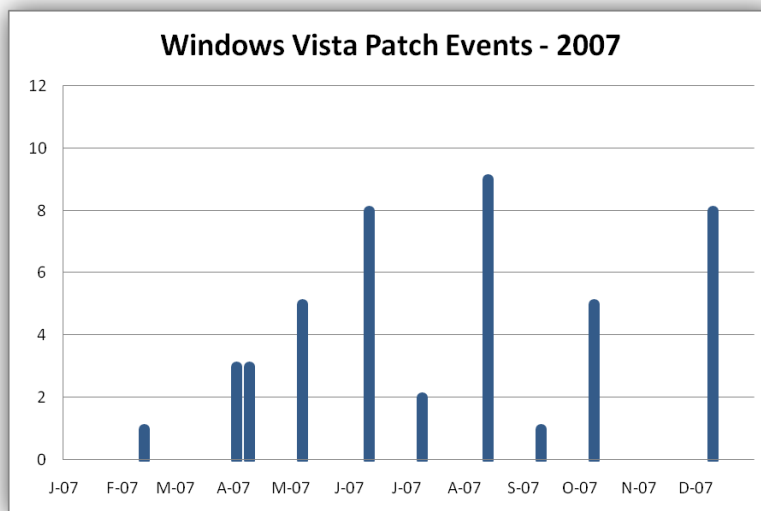
Windows XP has been in use for over six years now and in 2004, Microsoft released Windows XP SP2, a service pack focused on delivering some interim security improvements. Windows Vista delivers further improvements on that foundation, including things like ASLR and the ability for many more users to run as standard user (rather than admin), but clearly Windows XP SP2 presents a higher bar for improvement than the original (pre-SDL) release of Windows XP.

In the wake of my [Windows Vista One Year Vulnerability Report](#), I have received many questions regarding the current vulnerability record of Windows Vista as compares with Windows XP SP2.

This short paper is a compilation of vulnerability data for Microsoft Windows Vista and Microsoft Windows XP SP2 for calendar year 2007 and a brief analysis to see if any benefit is apparent for users of one OS over the other.

Windows Vista

During the calendar year of 2007, Microsoft released a total of 23 Security Bulletins in 10 different patch events that addressed 45 vulnerabilities in Windows Vista. The following figure charts the 52 weeks in 2007 and shows the patch events. The height of the bar is the number of vulnerabilities addressed.



The vulnerabilities were severity rated as follows by Microsoft:

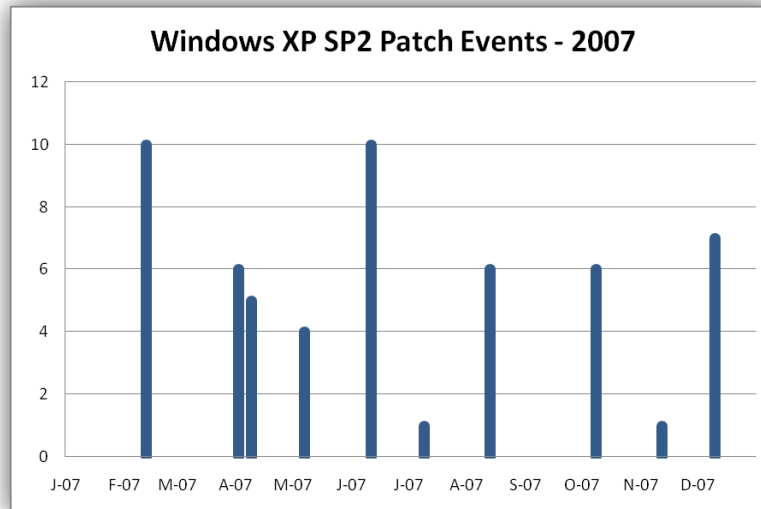
- Critical – 17 vulnerabilities
- Important – 19 vulnerabilities
- Moderate – 7 vulnerabilities
- Low – 2 vulnerabilities

Using the CVSSv2 ratings from the [NVD](#), the vulnerabilities were rated:

- High – 27 vulnerabilities
- Medium – 18 vulnerabilities

Windows XP SP2

During the calendar year of 2007, Microsoft released a total of 33 Security Bulletins in 10 different patch events that addressed 56 vulnerabilities in Windows XP SP2. The following figure charts the 52 weeks in 2007 and shows the patch events. The height of the bar is the number of vulnerabilities addressed.



The vulnerabilities were severity rated as follows by Microsoft:

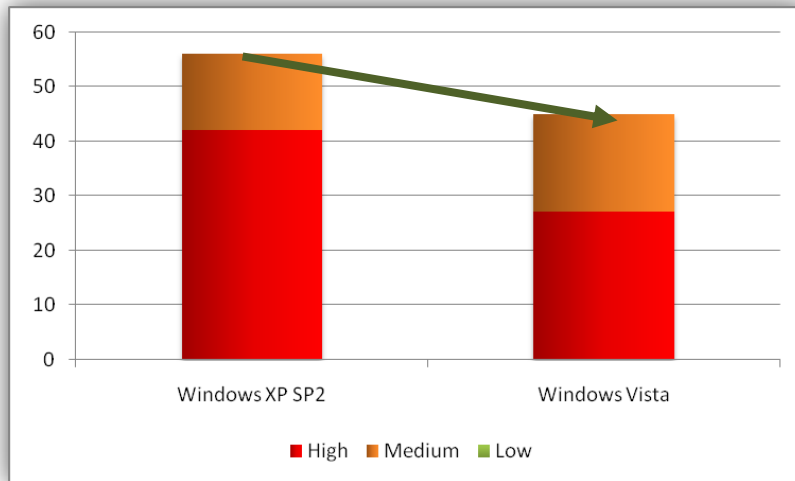
- Critical – 35 vulnerabilities
- Important – 15 vulnerabilities
- Moderate – 4 vulnerability
- Low – 2 vulnerabilities

Using the CVSSv2 ratings from the [NVD](#), the vulnerabilities were rated:

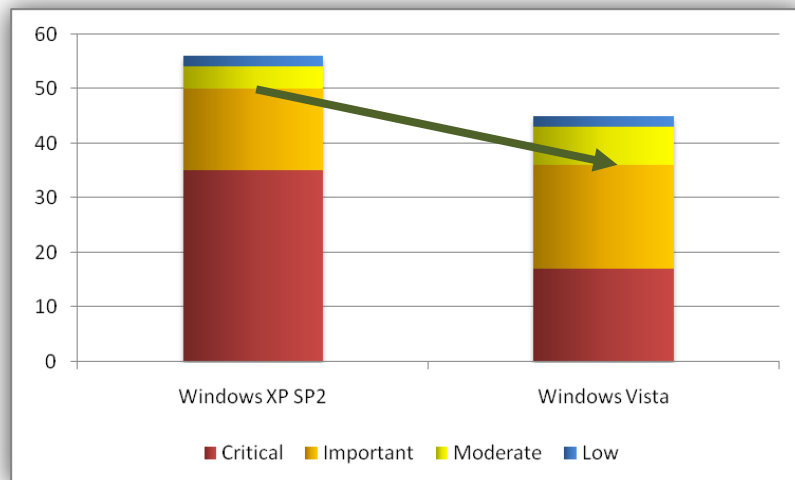
- High – 42 vulnerabilities
- Medium – 14 vulnerabilities

Summary

While both products had the same number of patch events (10) with Microsoft's monthly cycle, Windows XP SP2 users were affected by 43% more¹ Security Bulletins and 24% more vulnerabilities. Charting the vulnerabilities using the NVD ratings, we get the following:



Charting the vulnerabilities using the Microsoft ratings, we get the following chart:



¹ Windows XP SP2 had 24% more Security Bulletins and vulnerabilities than Windows Vista. Expressed relative to Windows XP SP2 instead, one could say that Windows Vista had 30% fewer Security Bulletins and 20% fewer vulnerabilities.

One other area that I was interested in examining was the impact of UAC. (NOTE: For a great discussion of UAC potential security value, read Crispin Cowan's [UAC: Desert Topping, or Floor Wax?](#))

As I've [discussed previously on my blog](#), I see the value of UAC as a mechanism that enables user to reasonable operate as non-admin. I adopted Windows Vista quickly on my home computer in order to leverage UAC. My wife, my daughter and I run full time in standard accounts. They don't know an admin password and have to get me to do admin stuff for them , which I do from a completely different admin account. Should my mind be more at ease knowing my family is running as standard users?

I examined each of the vulnerabilities that affected Windows Vista in 2007 to see if the impact was different for standard users. 26 out of the 45 Vista vulnerabilities, if successfully exploited, would grant rights as the logged on users. At the least, this means successful attackers will have to do some more work to gain elevated privileges beyond standard user.

My daughter is additionally limited in the web sites she can visit because of Parental Controls, so that would be an additional measure of protection, for those where an attacker lures victims to a malicious web page. I've summarized what I think are the 3 key scenarios in this table:

System / User Scenario	Impact / Mitigation
Windows XP SP2 users (typically running as admin)	If successfully exploited, attacker gains admin
Windows Vista non-admin (my wife)	If exploited, attacker does not gain admin
Windows Vista non-admin + Parental controls (my daughter)	Can't browse to web pages not on a pre-approved list, even if redirected/embedded

So in summary for Windows Vista and Windows XP SP2, I found that Windows Vista offers benefit over Windows XP SP2 in the following ways for 2007:

- Windows Vista had 30% fewer Security Bulletins than Windows XP SP2
- Windows Vista had 20% fewer vulnerabilities than Windows XP SP2
- Windows Vista had 28% fewer Critical and Important vulnerabilities than Windows XP SP2
- 26 vulnerabilities on Windows Vista are less severe for any users running as standard user.

Appendix A: Interpreting the Data

I think it worth spending a moment to discuss what this document covers, why it might be useful to some people and, perhaps most importantly, what it does not say.

If it was possible to measure "security" in one metric, it would have to encompass a complex combination of factors including (but not limited to) the software quality, administrative controls, physical controls, and much more – and even then, it would all be in the context of whatever security policy was defined for the systems in question.

So, this is not an analysis of "the security" of these operating systems. I don't look at protective mechanisms and see how they might protect in every scenario, or mitigate risk. Nor do I look at security features and see how they might enable better privacy or help secure business process. And I certainly don't look at how easy it is to manage the security policy for these products.

Is there anything in this analysis which will prove one piece of software is "more secure" than another? No, not really.

This report is a vulnerability analysis, which may provide some elements that could be **part of** a broader security analysis. I fundamentally believe that security and non-security features need to be built upon a foundation of good engineering and solid security quality if they are to perform as we expect and not be misused to the detriment of security.

So, how are the metrics relevant then? Acknowledging that one factor can't measure the absolute "security", we can still look at individual factors that contribute to improving security or making it easier to manage risk. Ask yourself:

All other things being equal, is it easier to mediate risk on a system that has 10 vulnerabilities in a year or one that has 100 vulnerabilities in a year? Which has a more negative impact on your security team and risk management process – deploying 10 security updates per year or deploying 100 security updates per year?

Note that individual metrics can even be mutually exclusive. For example, vendor policy could mandate a single security update per year which would definitely decrease the number of patches to deploy. However, that same policy would almost certainly mean that the exposure time for publicized issues would increase.

My own context for vulnerability analysis is to measure against the goal of reducing customer risk. To me, all other things being equal, fewer vulnerabilities make it easier to manage risk. All other things being equal, fewer patches mean more time to spend on other security projects to reduce risk.

Appendix B: Data Sources

The analysis in this report uses a set of data that has been compiled, customized and cross-checked using several sources of data available on the Internet:

- Microsoft Security Bulletins as published at <http://www.microsoft.com/technet/security/current.aspx> and associated web pages
- The National Vulnerability Database (NVD), a database superset of the Mitre CVE list (<http://cve.mitre.org>). The NVD is also sponsored by the US Department of Homeland Security and makes their data downloadable in an XML format at <http://nvd.nist.gov/download.cfm>.
- Many security websites were utilized for detailed verification and validation of vulnerability details, and especially dates for when the issue was first discussed publicly. Some of the most commonly utilized were: www.securityfocus.com, the Bugtraq mailing list, www.secunia.com, and www.securitytracker.com, but there were many others.

Leveraging these and many other sources, I compiled a database of vulnerabilities for the products analyzed.

Note that in this report, “disclosure” is used to mean broad and public disclosure and not any sort of private disclosure or disclosure to a limited number of people.