

H1 2008 Desktop OS Vendor Report

Vulnerabilities and Days of Risk

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



by

Jeffrey R. Jones
Security Guy
(and Microsoft Director)

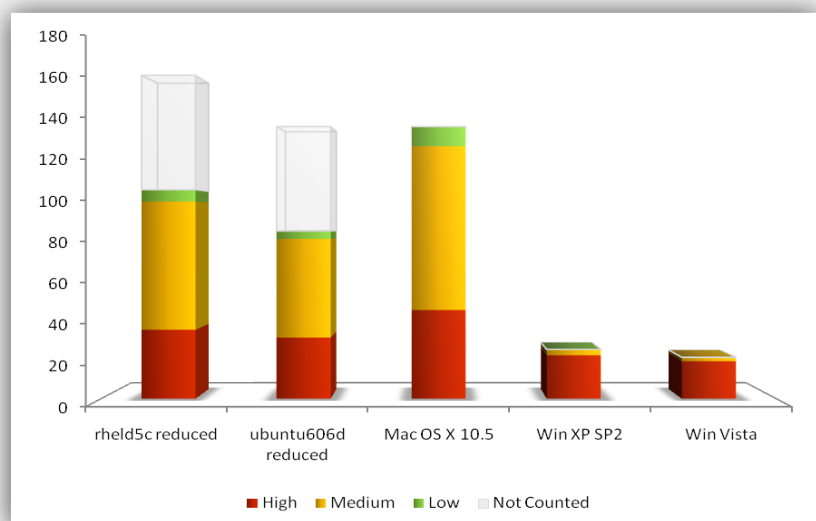
Windows Vista users saw the fewest vulnerabilities in 1H08 at 21, and experienced full or partial mitigation for 46% of the 26 vulnerabilities affecting Windows XP SP2 in 1H08.

This report looks at all of the vulnerabilities fixed by Apple, Microsoft, Red Hat and Ubuntu during the first half of 2008. At the vendor level, the report examines all vulnerabilities as well as *Days of Risk* (DoR) associated with those vulnerabilities. The report further drills down to examine just those issues affecting the commonly installed desktop operating system components.

The key findings for 1H08:

- The four vendors fixed a total 585 vulnerabilities in 1H08. 26.8% affected multiple vendors and of those, only 8 were fixed on the same day – the rest had an average 35 day delay between the first available fix and the last available fix..
- Microsoft had the lowest average Days of Risk for all vulnerabilities fixed at 24.22 days, with the next closest vendor at 72 days.
- For desktop OS vulnerabilities, Windows Vista had the fewest vulnerabilities in 1H08 at 21. The next lowest number was Windows XP SP2 at 26.
- Windows Vista customers experienced full or partial mitigation for 46% of the 26 vulnerabilities affecting Windows XP SP2 in 1H08, but also experienced one additional vulnerability in new code.

In addition to these measurements for the vendors and products, the body of the report also provides weighted analysis which provides a lesser consideration for lower severity issues. Please read the full report for details.



About the Author	3
Introduction	4
Charts and Analysis	5
Vendor Level View of Vulnerabilities.....	5
Combined View.....	5
Comparative View.....	7
Days of Risk by Vendor.....	9
Vulnerabilities by Product.....	11
Patch Events by Product.....	14
Detail by Vendor, Product	17
Microsoft.....	17
Windows XP SP2.....	18
Windows Vista.....	18
Windows XP SP2 Compared to Windows Vista.....	18
Apple.....	20
Mac OS X Leopard.....	21
Red Hat.....	21
Red Hat Enterprise Linux Desktop (v. 5 client).....	22
Ubuntu.....	22
Ubuntu 6.06 LTS (Desktop Edition).....	23
Summary.....	25
Appendix A: Interpreting the Data.....	26
Appendix B: Terms and Abbreviations	28
Appendix C: Data Sources.....	29
Appendix D: Methodology for “Reduced” Linux Desktop Configurations	30

About the Author

Jeff Jones is a Security 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 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 prior to that, the corporate McAfee anti-virus 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 focused on operating system security 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.

Introduction

In this report, I've tried to provide the analysis in a format that quickly delivers the interesting results, but then additionally provides greater levels of detail later in the document. Before drawing any final conclusions based upon the charts or data points, I strongly encourage you to read Appendix A: Interpreting the Data.

This report looks at vulnerability-related metrics for vulnerabilities fixed in desktop products during the first 6 months of 2008 by four vendors – Apple, Microsoft, Red Hat and Ubuntu. While this is not a comprehensive list of all possible desktop vendors, it does represent:

- Microsoft, provider of Windows software
- Red Hat, generally acknowledged the leading Linux distribution vendor, which offers long-term support
- Ubuntu, generally considered the most popular up and coming Linux distribution, which also offers long-term support.
- Apple, provider of Mac OS X

While there may be other desktop operating system vendors of interest to you, I believe this covers the ones of most interest to the majority. If you think there is a compelling reason to add another vendor or product, post a comment to me on my blog.

The rest of the report is broken into two large sections, followed by the Appendices. Briefly, these sections cover:

- Charts and Analysis. This section jumps directly into analysis of the final numbers and provides charts that look at several scenarios:
 - The set of combined vulnerabilities fixed in 1H08 by all vendors, including a combined view and individual vendor totals.
 - Days of Risk (DoR) values for each vendor in 1H08.
 - Vulnerability counts by desktop product, including severity analysis and views that weight the vulnerabilities based upon severity.
 - *Patch Events* by desktop product for 1H08.
- Vendor and Product Detail. This section will drill down into vendor and product specific vulnerability data points.

As additional context, I encourage you to review the section covering industry vulnerability trends in the latest Microsoft Security Intelligence Report (SIR), which can be found at <http://www.microsoft.com/sir>.

Charts and Analysis

Vendor Level View of Vulnerabilities

This section will look at the full set of vulnerabilities fixed by all of the vendors during the first half of 2008. In total, the four vendors fixed 585 vulnerabilities from January to June. Note that these include fixed vulnerabilities for all products for which the vendor released a security advisory¹ and provided a fix.

Each of these vendors identified vulnerabilities in their security advisories by CVE² identifiers, which were used to enumerate and analyze the sets of vulnerabilities. For analysis of other factors such as severity, the report utilizes information from the National Vulnerability Database (NVD), as published by the National Institute of Standards (NIST) at <http://nvd.nist.gov>.

Combined View

Figure 1 breaks down the vulnerabilities by vendor and highlight the intersection sets of vulnerabilities addressed by more than one vendor. No vulnerability affected all four vendors, but there were several intersection sets of vulnerabilities that affected more than one vendor.

¹ See Appendix C: Data Sources for links to each vendor's security advisories.

² Common Vulnerabilities and Exposures. See Appendix B: Terms and Abbreviations for more information.

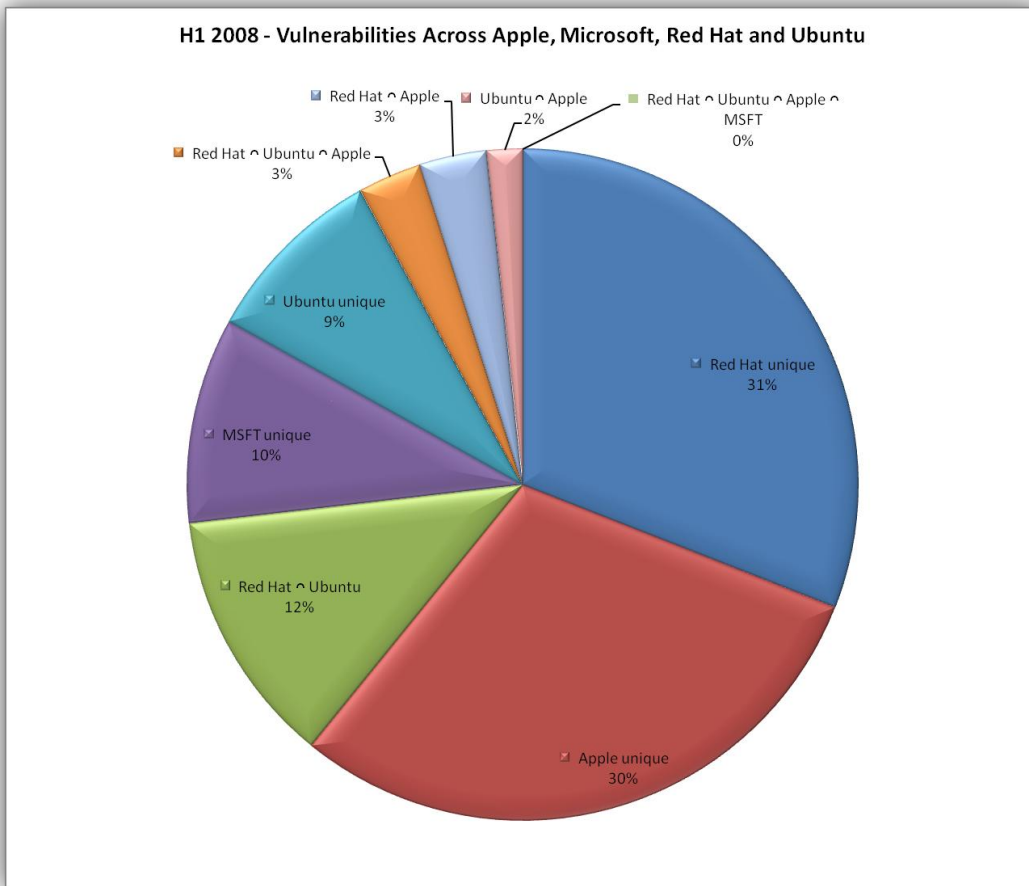


FIGURE 1. 1H08 COMBINED VIEW OF VULNERABILITIES FROM APPLE, MICROSOFT, RED HAT AND UBUNTU

When viewing the chart in Figure 1, one would need to combine all sections that apply to an individual vendor in order to get a total percentage affecting that vendor (and because of the intersections, they would add to more than 100%).

Out of the 585 vulnerabilities fixed by the vendors from January through June, 157 (26.8%) of vulnerabilities were fixed by more than one vendor in the period³.

- **Apple, Red Hat and Ubuntu.** There were eighteen vulnerabilities fixed commonly by Apple, Red Hat and Ubuntu during H1. For the set of vulnerabilities shared by all three vendors, Ubuntu was the first to provide a fix eight times. At the other end, Apple was last to provide a fix eleven times. The average delta between the first vendor to fix and the last vendor to fix is 73 days for the set of vulnerabilities common to all three.
- **Apple and Red Hat.** There were nineteen vulnerabilities fixed commonly by Red Hat and Apple. Red Hat was the first to provide a fix for 58% of these vulnerabilities. The average delta between the vendor fixes was approximately 30 days.

³ I did not cross-reference the H1 set of vulnerabilities against issues that were fixed by the vendors before this period. There may be more vulnerabilities common to the vendors, where one or more vendors fixed the issue prior to H1.

- *Apple and Ubuntu.* There were ten vulnerabilities fixed commonly by Apple and Ubuntu and of these, Ubuntu provided the first fix 60% of the time. The average delta between vendor fixes was approximately 39.6 days.
- *Red Hat and Ubuntu.* There were seventy-two vulnerabilities fixed commonly by Red Hat and Ubuntu. Red Hat was the first to provide a fix 66.6% of the time for this set of vulnerabilities and the average delta between the vendor fixes was approximately 28.5 days.

Only 8 out of the 157 common vulnerabilities were addressed by the vendors on the same day. The largest delta between vendor fixes for the same issue was 180 days, almost the length of the entire period³. On average, there was about 35.5 days between the first vendor fix and the last vendor fix.

Comparative View

Figure 2 shows all vendor vulnerabilities broken down by severity for 1H08.

It would be nice to look at how many “products” contribute to each vendors total, but it is impractical, as each of the vendors effectively support several products and technologies, but with very different levels of bundling.

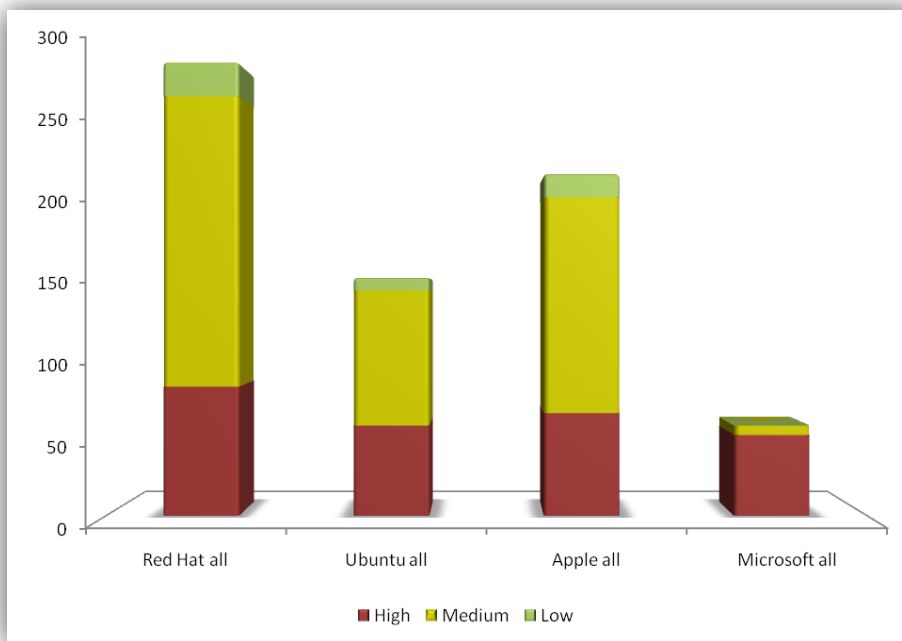


FIGURE 2. 1H08 VULNERABILITIES BY VENDOR, SEVERITY

The total number of vulnerabilities in the charts is: Red Hat 292; Ubuntu 153; Apple 222; and Microsoft 58.

While the stack chart of Figure 2 effectively gives one the ability to compare vulnerabilities by severity from each vendor, some might assert that stacking vulnerabilities in the chart could skew the observer’s perception to place more significance on lower severity issues than is warranted.

To address this concern, I also created a “weighted” view of the H108 vendor vulnerability data, leveraging the weighting values established by NIST in their Vulnerability Workload Index (VWI)⁴. Essentially, the Figure 3 is a weighted chart that takes severity into account, using (High/1), (Medium/5) and (Low/20) as a weighting factor.

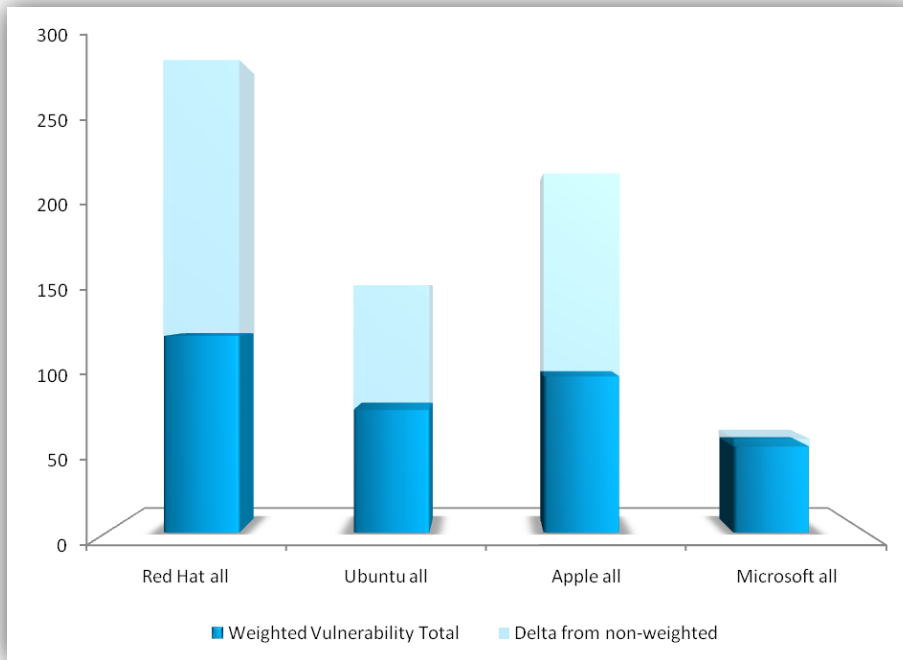


FIGURE 3. WEIGHTED VULNERABILITY TOTALS BY VENDOR FOR 1H08

This weighting basically creates a view where it takes 20 Low severity vulnerabilities or 5 Medium severity vulnerabilities to equal one single High severity vulnerability. This table summarizes how the weighted analysis changes the totals for each vendor.

TABLE 1. WEIGHTED VS. NON-WEIGHTED VULNERABILITY TOTALS

Vendor	Total vulnerabilities	Weighted value
Red Hat	292	121.5
Ubuntu	153	75.8
Apple	222	96.5
Microsoft	58	53.2

⁴ Read more about the Vulnerability Workload Index at <http://nvd.nist.gov/home.cfm?workloadindex>.

Days of Risk by Vendor

Days of risk (DoR) is a metric that I believe is best measured at the vendor level across all products, since it is aimed at measuring how the combination of vendor policy, resources and decision making combine to enable a vendor to provide a fix to address a publicly disclosed vulnerability. I refer to the time from when vulnerability is public disclosed until a fix is made available from the vendor as a *DoR window* or window of exposure.

Publicly disclosed, in the context of this report, means broadly known to a potentially large set of attackers due to discussion in a publicly available document or web site – typically Bugtraq, a bugzilla site, or similar. The public disclosure of a vulnerability greatly increases the pool of potential attackers that could develop exploits against target customers. To see more detail on assumptions made when calculating DoR, read Appendix A: Interpreting the Data.

The chart in Figure 4 shows the average DoR for all⁵ of the vulnerabilities the vendors fixed in 1H08.

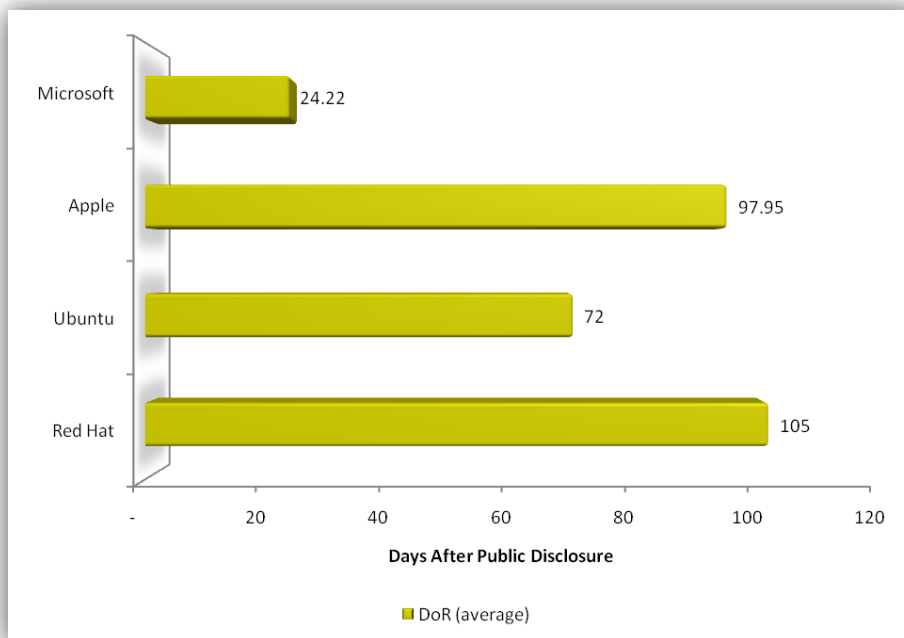


FIGURE 4. AVERAGE DAYS-OF-RISK BY VENDOR FOR 1H08

Calculating the average DoR for each vendor, Microsoft had the lowest average DoR at 24.22 days and Red Hat had the highest average at 105 days. Again, though, this level of analysis gives equal weighting to Low and High severity issues. This means if a vendor gives a much high priority to High severity issues, the DoR exposure windows for Low severity issues could be skewing these averages negatively with respect to severity, a factor commonly used by customers for prioritization.

⁵ Note that for Red Hat, I excluded some vulnerabilities for products where I couldn't definitively nail down certain information. However, all supported Red Hat Enterprise Linux operating system products and associated components are included. See more detail in the Detail subsection on Red Hat Enterprise Linux Desktop (v. 5 client).

To accommodate severity, I again developed a weighted view using the same weighting factors as before, decreasing the impact of Medium severity issues by a factor of 5 and decreasing the impact of Low severity issues by a factor of 20.

Figure 5 shows the weighted chart that takes severity into account, using (High/1), (Medium/5) and (Low/20) as a weighting factor for calculating DoR.

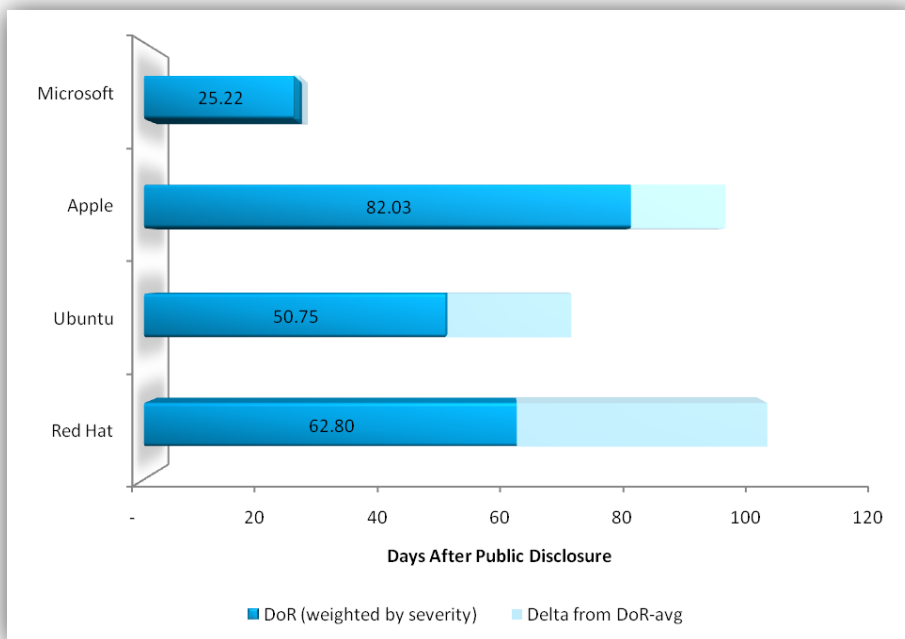


FIGURE 5. WEIGHTED AVERAGE DAYS-OF-RISK BY VENDOR FOR 1H08

Taking the severity weighting into account, we again see that on average, Microsoft provides fixes for publicly disclosed issues faster than the other vendors by a pretty significant margin.

However, note how the weighted chart displays some pretty telling differences from the unweighted DoR chart for the other vendors. The longest weighted DoR is now Apple. Given the deltas displayed on the chart, for example, we can conclude that Red Hat addresses High severity issues much more quickly than lower severity issues, while Apple has less of a difference in DoR between how quickly they address High severity and lower severity issues – both are relatively longer DoR windows. This confirmed in Table 2. 1H08 Days-of-Risk Summary, All Vendors.

TABLE 2. 1H08 DAYS-OF-RISK SUMMARY, ALL VENDORS

DoR Data Points	Apple	Microsoft	Red Hat	Ubuntu
avg DoR	97.6 days	24.2 days	105 days	72 days
avg DoR (High)	70.6 days	25.5 days	37.5 days	42.02 days
Median DoR	17 days	0 days	16 days	20 days
Median DoR (High)	15 days	0 days	0 days	7 days
Percentage fixed with 1 day or less	17%	89.7%	38%	23.5%

of public disclosure				
Percentage fixed in 1 day or less of public disclosure (High)	17%	90.3%	60%	20.7%
Longest DoR window ⁶	1001 days	495 days	1292 days	623 days

Vulnerabilities by Product

In this section, we shift from analyzing all vulnerabilities fixed by the vendor to just those affecting the most recently released desktop product from the vendor, with the following caveats:

- I include Windows XP SP2 in addition to Windows Vista, due to interest expressed by the public⁷
- I include only versions for which the vendor offers long term support, a condition required by most businesses to consider the product for deployment. This mostly affects Ubuntu, which also ships versions that do not have long term support.
- I include the most recent version that was available for the full period of 1H08. If a product shipped in the middle of the period, I'll cover it in a future study.

Taking these caveats into account, this means I examined (see

⁶ I validated the dates for public disclosure against the dates published by Red Hat in the `cve_date.txt` file from <http://www.redhat.com/security/data/metrics/>.

⁷ My measure of this interest comes from both questions directed to me on my blog, as well as the number of stories published with respect to Windows XP SP2 in 1H08.

Detail by Vendor, Product for more information) for the following products:

- Windows Vista
- Windows XP SP2
- Mac OS X Leopard
- Red Hat Enterprise Linux Desktop (v5. Client)
- Ubuntu 6.06 LTS

Figure 6 charts all vulnerabilities fixed for each respective product as documented in a security advisory in 1H08.

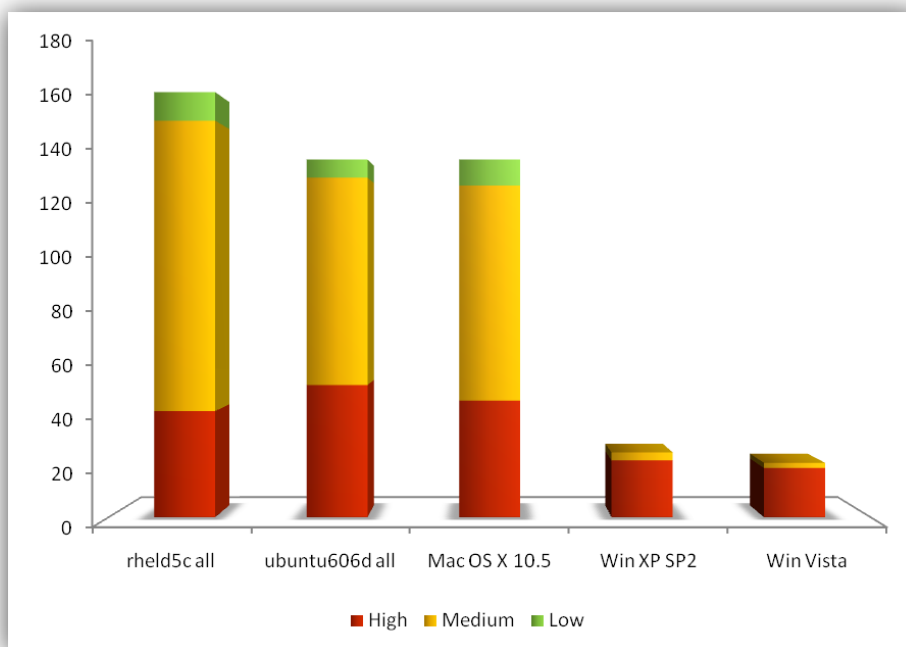


FIGURE 6. H108 VULNERABILITIES BY PRODUCT, SEVERITY

The above chart includes vulnerabilities from all components supported by the vendor as part of the product. In this view, Windows Vista had the fewest vulnerabilities and rheld5c had the most.

Vendors vary widely in what they bundle into a product – typically to gain a competitive advantage or support a business plan for the product. However, along with the business advantage gained by bundling in a lot of functionality is the security disadvantage of having more components that could have a vulnerability and potentially expose customers.

From the most conservative security viewpoint, the fact that some user *may* have some of the optional components installed means that Figure 6 is the view of vulnerabilities which they have to worry about if they've deployed that particular product.

However, a common objection to comparisons that take the most conservative security viewpoint is that Linux distributions include many optional components not installed by default that would not be *commonly* installed on the average user's desktop. I don't disagree, and I am interested in a view that presents a view of more comparable configurations.

With that in mind, I created reduced configurations for the two Linux desktop operating systems and excluded any vulnerabilities from (a) optional components that were not installed by default and (b)

OpenOffice and a couple of graphics components⁸. The chart showing this reduced view is shown in Figure 7.

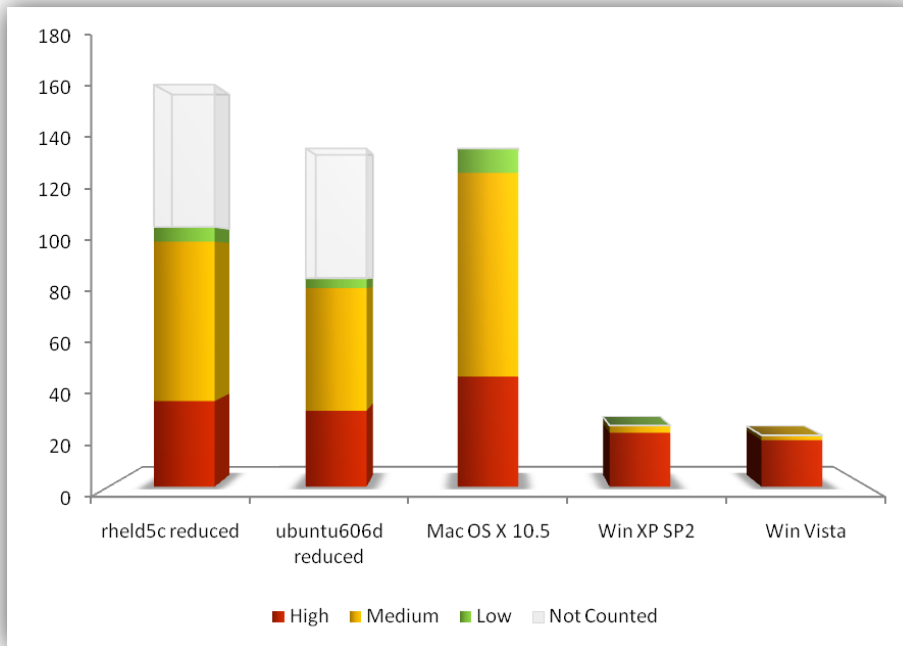


FIGURE 7. H108 VULNERABILITIES BY PRODUCT, SEVERITY (REDUCED LINUX CONFIGURATIONS)

Similar to when we looked at all of the vulnerabilities from the vendors, the stack chart of Figure 7 gives one the ability to compare vulnerabilities by severity for each product, but applying the same arguments as above, I also wanted to see a view with weight applied for severity.

As I did with previous charts, I created a weighted view of the H108 product vulnerability data, leveraging the weighting values established by NIST in their VWI. Figure 8 is a weighted chart that takes severity into account, using (High/1), (Medium/5) and (Low/20) as a weighting factor for the product vulnerabilities.

⁸ If you are interested in the detail, you can get more information in the product sections later in the document as in Appendix D: Methodology for "Reduced" Linux Desktop Configurations.

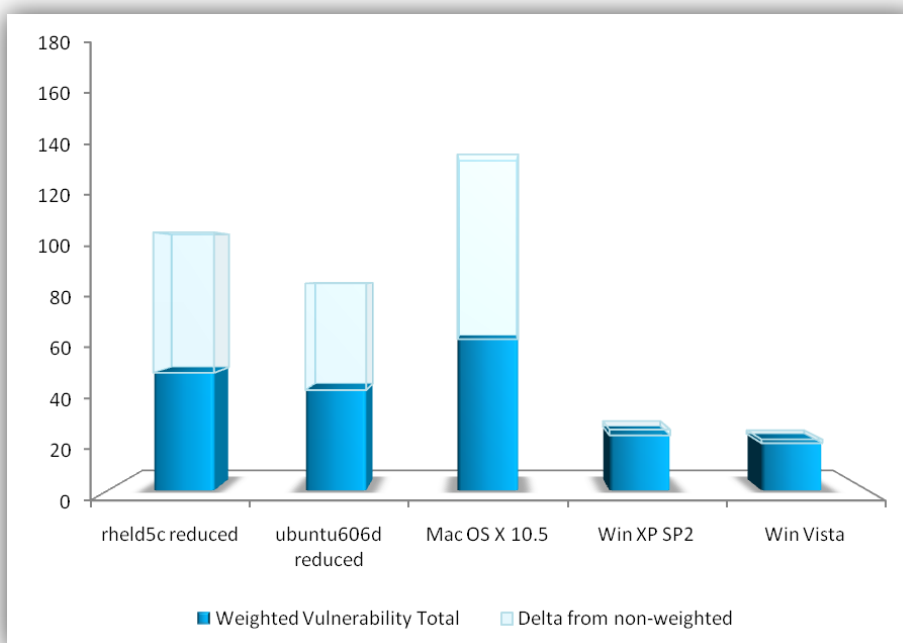


FIGURE 8. WEIGHTED VULNERABILITY TOTALS BY PRODUCT FOR 1H08

Windows Vista still had the lowest weighted value for 1H08, roughly 18% lower than the Windows XP SP2 and over 50% lower than the next closest product, the reduced build of Ubuntu 6.06. Mac OS X Leopard had the highest weighted value for vulnerabilities in the period.

Patch Events by Product

As I've discussed metrics with enterprise customers in the past, I discovered that there is another view of vulnerability fixes that is important to them – "how often did we have to get our team together to assess, test and roll out a set of updates?" They also wanted enough time between releases that they could make reasonable progress in rolling out a set of updates.

This direct feedback from customers is what led to Microsoft moving to a monthly, predictable update release process. After that change, I came up with Patch Events⁹ as a way to measure the impact on security teams over a period, to look at impact before and after.

In this section, I chart the Patch Events for each desktop product analyzed in the report, giving a visual view of the impact. The height of the bars is the number of vulnerabilities fixed during an event (and color coded), while the individual Patch Events are graphed according to the date they occurred.

⁹ I define "Patch Event" as any day on which one or more security fixes are released.

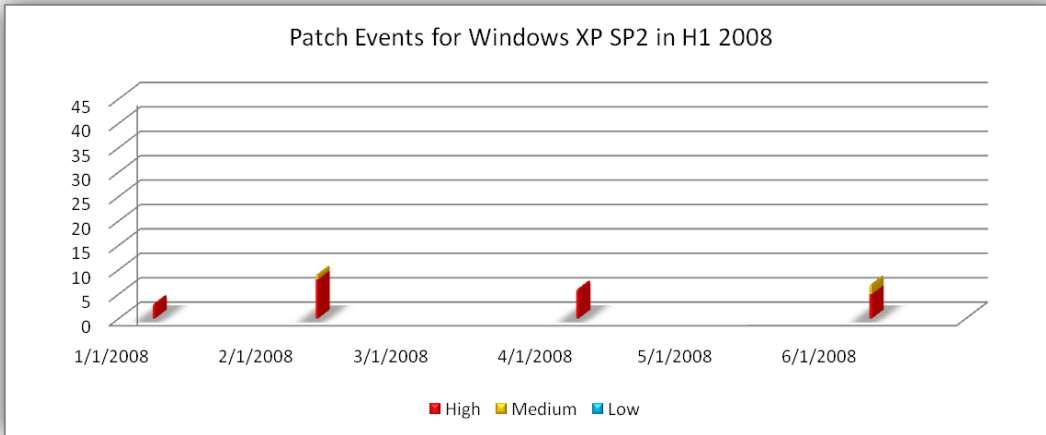


FIGURE 9: WINDOWS XP SP2 VULNERABILITIES IN H1 2008 (BY PATCH EVENT, SEVERITY)

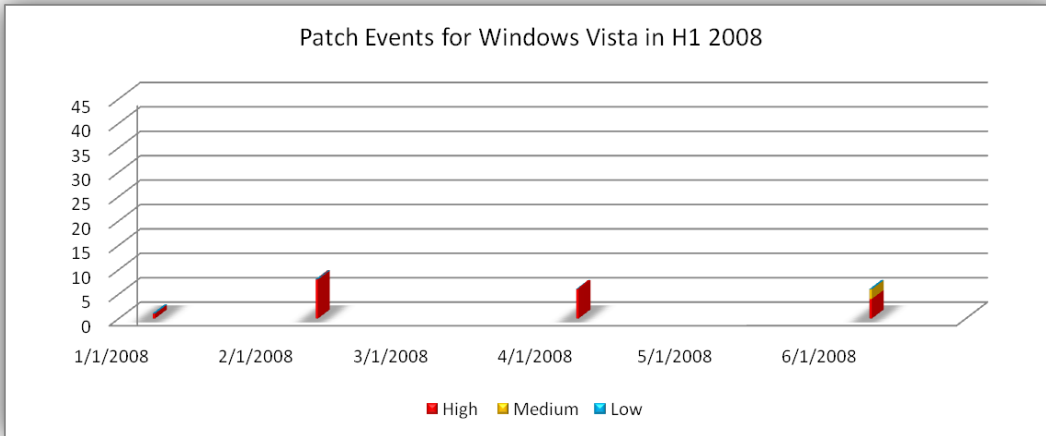


FIGURE 10. WINDOWS VISTA VULNERABILITIES IN H1 2008 (BY PATCH EVENT, SEVERITY)

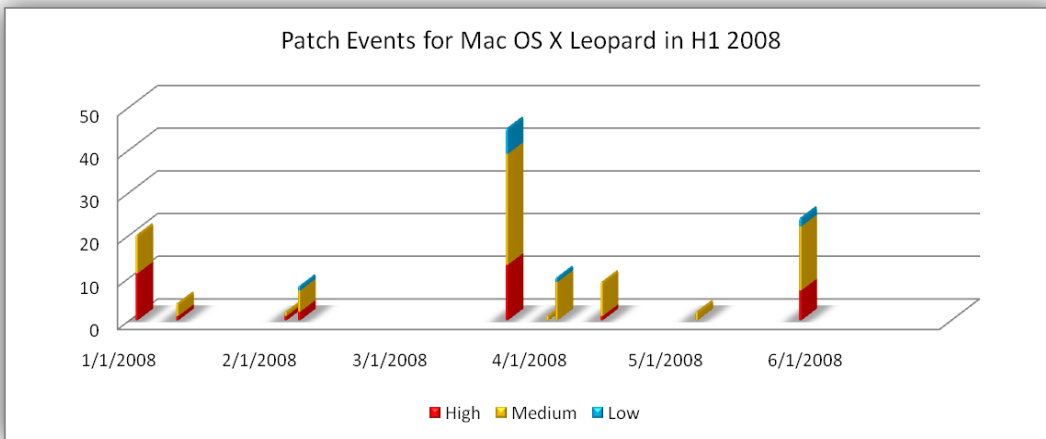


FIGURE 11: MAC OS X LEOPARD VULNERABILITIES IN H1 2008 (BY PATCH EVENT, SEVERITY)

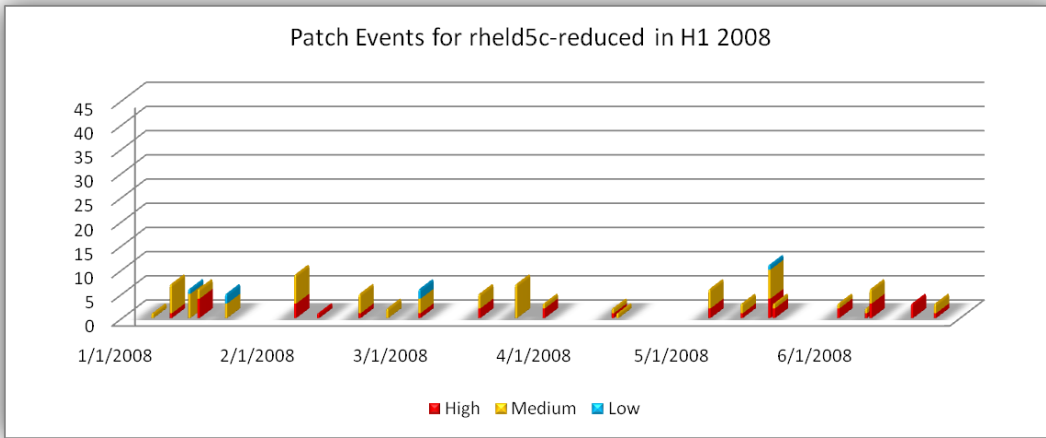


FIGURE 12: RHELD5C-REDUCED VULNERABILITIES IN H1 2008 (BY PATCH EVENTS, SEVERITY)

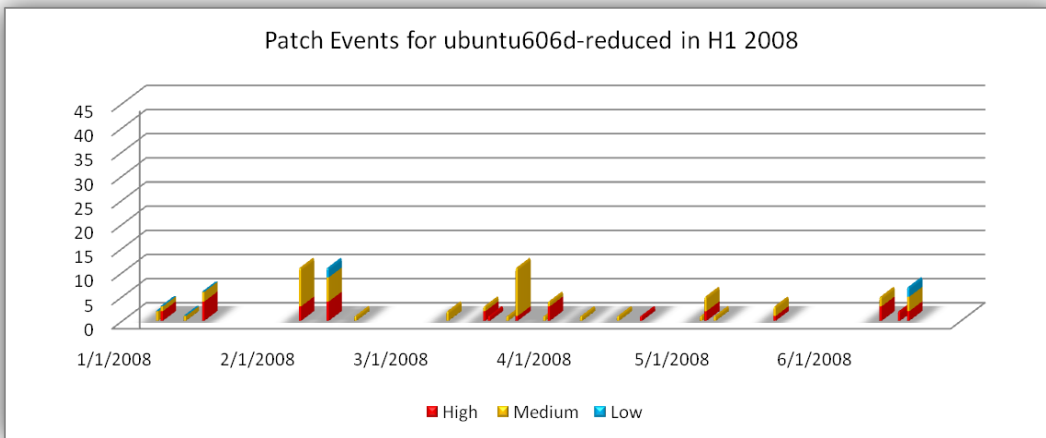


FIGURE 13: UBUNTU606D-REDUCED VULNERABILITIES IN H1 2008 (BY PATCH EVENTS, SEVERITY)

Detail by Vendor, Product

Microsoft

Across all products¹⁰, Microsoft released 36 Security Bulletins during six Patch Events addressing 58 vulnerabilities in 1H08. The 58 vulnerabilities addressed by Microsoft in the period had an average DoR of 24.22 days and the median DoR window of exposure was 0 days. Roughly 90% of all vulnerabilities were fixed within 1 day of public disclosure. Other key data points are summarized in Table 3.

TABLE 3: MICROSOFT DoR DATA POINTS

Key data points	Value	Notes
avg DoR	24.22 days	average for 58 vulnerabilities
avg DoR (High)	25.5 days	average for 52 vulnerabilities rated High by nvd.nist.gov
Median DoR	0 days	
Median DoR (High)	0 days	
Percentage fixed with 1 day or less of public disclosure	89.7%	52 out of 58
Percentage fixed with 1 day or less of public disclosure (High)	90.3%	47 out of 52 High
Longest DoR window	495 days	CVE-2007-0675, an issue in the Microsoft Speech API, rated High by nvd.nist.gov . Microsoft rated the issue Moderate on desktop OSes and Low on server OSes.

Key events that occurred during 1H08:

- Microsoft released Windows Vista SP1 in February 2008.
- Microsoft released Windows XP SP3 in May 2008.

¹⁰ These numbers represent Security Bulletins and vulnerabilities released for all Microsoft products, not just those related to operating systems.

- June 30, 2008 was the “end of sale” date for Windows XP. Security updates will continue through April of 2014.

Windows XP SP2

Windows XP SP2 is a currently supported desktop operating system originally released nearly seven years ago in October of 2001. SP2 was a security-focused service pack update released approximately four years ago in August 2004.

From January to June of 2008, Microsoft issued 19 Security Bulletins during 4 Patch Events addressing 26 vulnerabilities in Microsoft XP SP2. 22 of those vulnerabilities were rated High severity. This is down 9 (25%) from 1H07, when Windows XP SP2 had 35 vulnerabilities.

Windows Vista

Windows Vista is the most recent desktop operating system from Microsoft, released to business customers in November 2006.

From January to June of 2008, Microsoft issued 16 Security Bulletins during 4 Patch Events addressing 21 vulnerabilities in Windows Vista, of which 19 were rated High severity. This is up one (5%) from 1H07, when Windows Vista had 20 vulnerabilities.

Windows XP SP2 Compared to Windows Vista

Windows XP SP2 was a security-focused service pack and Windows Vista is its successor, a release that benefitted more fully from security architecture improvements and the Microsoft Security Development Lifecycle (SDL). Many people have expressed interest in how they compare in terms of vulnerabilities.

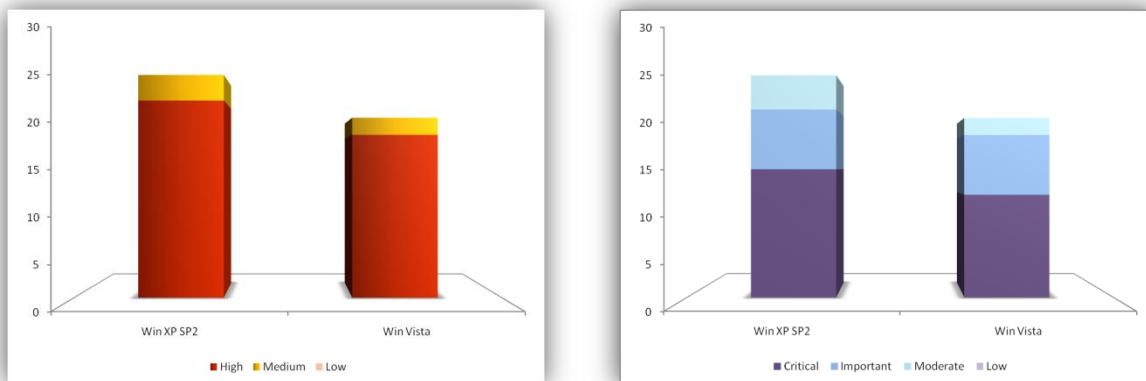


FIGURE 14. 1H08 VULNERABILITIES FOR WINDOWS XP SP2 AND WINDOWS VISTA, BY NVD SEVERITY (LEFT) AND MSRC SEVERITY

Figure 14 shows Windows XP and Windows Vista vulnerabilities for 1H08 charted side-by-side and broken down by NVD severity ratings. Windows XP had 24% more vulnerabilities than Windows Vista and 21% more High severity vulnerabilities.

However, this summary doesn’t answer some questions. How many vulnerabilities were newly introduced in Windows Vista? How many vulnerabilities were mitigated or removed by the Security Development Lifecycle process for Windows Vista?

I examined each of the vulnerability details for those affecting Windows XP or Windows Vista and found the following:

- 1 vulnerability affected Windows Vista that did not affect Windows XP SP2. CVE-2008-0084 was a vulnerability in TCP/IP that could be used for denial-of-service by a specially crafted DHCP server. This was in the new networking stack for Windows Vista.
- 2 of the vulnerabilities affecting both Windows Vista and XP SP2 had lower severity on Windows Vista.

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 reasonably operate as standard user (not 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 to see if the impact was different for standard users. If so, a successful exploitation 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 automatically gains admin and therefore has greater potential impact
Windows Vista non-admin (my wife)	If exploited, attacker does not gain admin, so impact is limited
Windows Vista non-admin + Parental controls (my daughter)	Can't browse to web pages not on a pre-approved list, even if redirected/embedded, further reducing risk of exploitation

Examining the 21 vulnerabilities affecting Windows Vista in 1H08, I found that the UAC benefit applies to 6 vulnerabilities - where customers run as standard user, the system risk is reduced.

To summarize, Windows Vista customers experienced full or partial mitigation for 46% of the 26 vulnerabilities affecting Windows XP SP2 in 1H08, but also experienced one additional vulnerability introduced in new code. This is shown graphically in Figure 15.

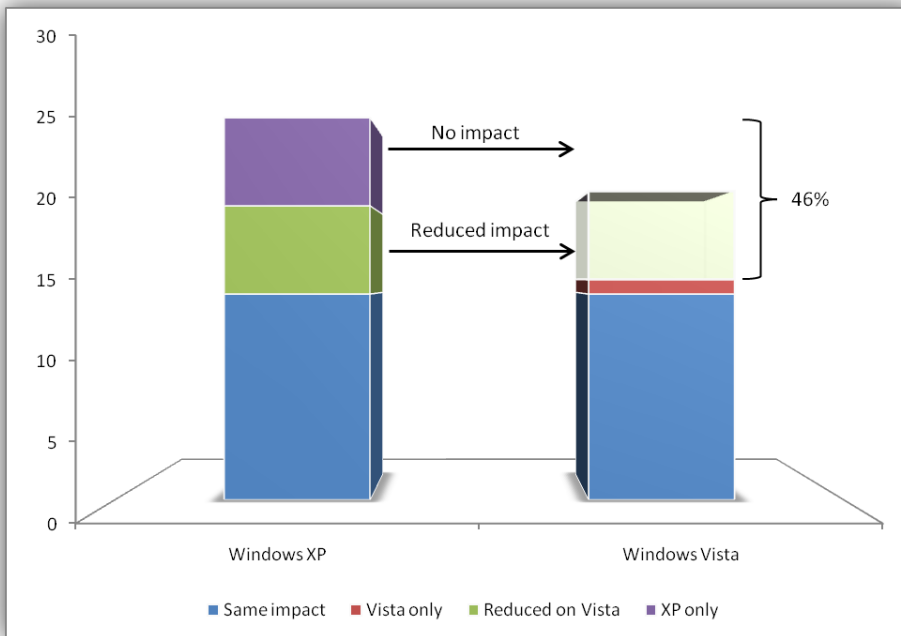


FIGURE 15. IMPACT REDUCTION BENEFIT OF WINDOWS VISTA IN 1H08

Apple

Across all products, Apple released 15 advisories during 13 Patch Events addressing 222 vulnerabilities in H1 2008.

The 222 security vulnerabilities addressed by Apple in the period had an average DoR of 97.95 days and the median DoR windows was 17 days. Other key DoR data points are summarized in Table 4.

TABLE 4: APPLE DoR DATA POINTS

Key data points	Value	Notes
avg DoR	97.95 days	average for 222 vulnerabilities
avg DoR (High)	70.6 days	average for 68 vulnerabilities rated High by nvd.nist.gov
Median DoR	17 days	
Median DoR (High)	15 days	
Percentage fixed with 1 day or less of public disclosure	17%	38 out of 222
Percentage fixed in 1 day or less of public disclosure (High)	17%	12 out of 68 High
Longest DoR window	1001 days	CVE-2005-3164, a Low severity issue in Mac OS X Tiger

Mac OS X Leopard

Apple's latest desktop operating system, Mac OS X Leopard (10.5.x) became generally available to customers on October 26, 2007.

During the period from January to June 2008, Apple released 13 advisories during 11 Patch Events addressing 138 vulnerabilities. 45 of the 138 were rated High severity.

Red Hat

Across all products, Red Hat released 137 advisories during 55 Patch Events addressing 292 vulnerabilities in H1 2008.

Note: For certain calculations, I did not have enough information concerning general availability dates for several of the products like Red Hat Network Proxy, Server and similar, so I filtered down to just issues affecting the Red Hat Enterprise Linux operating systems.

However, administrators may want to examine security advisories and vulnerabilities for the non-OS products in more detail, as the 95 CVEs I excluded were some of the oldest - including 20 that have been publicly disclosed for over two years and an additional 19 that have been publicly disclosed for over one year.

After excluding vulnerabilities for the reasons described above, 197 vulnerabilities remained that affected one of the Red Hat Enterprise Linux desktop or server OS products. These 197 security vulnerabilities addressed by Red Hat in the period had an average DoR exposure window of 105 days and the median DoR exposure window was 16 days. Other key DoR data points are summarized in

Table 5.

TABLE 5: RED HAT DoR DATA POINTS

Key data points	Value	Notes
avg DoR	105 days	average for 197 vulnerabilities affecting RHEL desktop and server products
avg DoR (High)	37.5 days	average for 48 vulnerabilities rated High by nvd.nist.gov
Median DoR	16 days	median for 197 vulnerabilities affecting RHEL desktop and server products
Median DoR (High)	0 days	median for 48 vulnerabilities rated High by nvd.nist.gov
Percentage fixed with 1 day or less of public disclosure	38%	74 out of 197
Percentage fixed in 1 day or less of public disclosure (High)	60%	28 out of 48 High

Longest DoR window ¹¹	1292 days	CVE-2007-6206, a Low severity issue affecting the 2.4 and 2.6 Linux kernel
----------------------------------	-----------	--

Key Events for Red Hat in 1H08:

- On 6/3/2008, Red Hat sent out [RHSA-2008:0521](#) notifying customers that Red Hat Enterprise Linux 2.1 would reach end of life on May 31, 2009 (ending 7 years of support).

Red Hat Enterprise Linux Desktop (v. 5 client)

The newest version of Red Hat’s Enterprise Linux desktop offering is Red Hat Enterprise Linux Desktop (v. 5 client), which I will abbreviate as rheld5c. Red Hat issued 55 security advisories during 35 patch events addressing 164 vulnerabilities in rheld5c during H1 2008.

However, as is typical for Linux distributions, rheld5c contains many optional components that would not commonly be installed on a typical desktop, including many server applications. For that reason, I filtered out all vulnerabilities for optional components not installed during a default installation, plus a few default components that do not have a comparable component on a Microsoft Windows OS (see Appendix D: Methodology for “Reduced” Linux Desktop Configurations, for details.) I will refer to this reduced subset of rheld5c as rheld5c-reduced.

Red Hat issued 28 security advisories during 27 Patch Events addressing 106 vulnerabilities in rheld5c-reduced, so the exclusion of optional components eliminates about 35% of vulnerabilities from the analysis. 35 of the 106 were rated High severity.

Ubuntu

Across all products, Ubuntu released 78 advisories during 47 Patch Events addressing 153 vulnerabilities in H1 2008.

Note: Ubuntu does a good job of publishing original advisories and regression advisories. I did not count the regression advisories in my count above unless a new, unique vulnerability was being addressed or a fix was announced for an additional platform or package.

For example, usn-612-1, usn-612-2 and usn-612-3 were all released on the same day addressing CVE-2008-0166 in different packages and platforms. Usn-612-4 addresses the same vulnerability in an additional package the next day. Usn-612-7 addresses one package from usn-612-1, but as part of a different product. I counted each of these.

In contrast, usn-612-6 addressed a regression bug from usn-612-3 and I didn’t count this as a separate security advisory.

These 153 security vulnerabilities addressed by Ubuntu in the period had an average DoR of 72 days and the median DoR window was 20 days. Other key DoR data points are summarized in Table 6.

TABLE 6: UBUNTU DoR DATA POINTS

¹¹ I validated the dates for public disclosure against the dates published by Red Hat in the `cve_date.txt` file from <http://www.redhat.com/security/data/metrics/>.

Key data points	Value	Notes
avg DoR	72 days	average for 153 vulnerabilities affecting Ubuntu products
avg DoR (High)	42.02 days	average for 58 vulnerabilities rated High by nvd.nist.gov
Median DoR	20 days	median for 153 vulnerabilities affecting Ubuntu products
Median DoR (High)	7 days	median for 58 vulnerabilities rated High by nvd.nist.gov
Percentage fixed with 1 day or less of public disclosure	23.5%	36 out of 153
Percentage fixed in 1 day or less of public disclosure (High)	20.7%	12 out of 58 High
Longest DoR window	623 days	CVE-2007-6206 , a Low severity issue affecting the Linux kernel

Key Events for Ubuntu in H1 2008:

- Ubuntu released Ubuntu 8.04 LTS (Hardy Heron)¹² on April 21, 2008, the first new release for which they offer Long-Term Support¹³ since Ubuntu 6.06 LTS.
- Ubuntu support for Ubuntu 6.10 (Edgy Eft) reached end of life¹⁴ on April 25, 2008, signaling that no further security fixes will be produced. This was as planned, since non-LTS versions are supported roughly 18 months.

Ubuntu 6.06 LTS (Desktop Edition)

Ubuntu releases are packaged into Desktop and Server editions, with installation packages optimized towards a default set of components appropriate to the respective role. In this section, I examine the vulnerabilities affecting the Desktop edition, which I will abbreviate as ubuntu606d.

Note: I anticipate getting the question of why Ubuntu 6.60 LTS and not one of the subsequent versions like 6.10, 7.04, 7.10, or 8.04 LTS . The simple answer is that I am looking at the most recent version for which

¹² See [Ubuntu 8.04 LTS Desktop Edition Released](#).

¹³ The "LTS" versions of Ubuntu receive long-term support. 3 years for desktop versions and 5 years for server versions.

¹⁴ See [End of Life announcement for Ubuntu 6.10](#).

Canonical offers enterprise-level, or in their terms, long term support, that was available for all of H1 2008. Ubuntu 8.04 LTS only shipped in April, while Ubuntu 6.10 reached its end of life in April and Ubuntu 7.04 will be reaching its end of life in October.

I believe that IT decision makers require long term stability and support in order to seriously consider an OS for production, so I do not focus on the non-LTS releases.

Ubuntu issued 54 security advisories during 35 patch events addressing 138 vulnerabilities in ubuntu606d during H1 2008.

However, as is typical for Linux distributions, ubuntu606d contains many optional components that would not commonly be installed on a typical user desktop, including many server applications. For that reason, I filtered out all vulnerabilities for optional components not installed during a default installation, plus a few default components that do not have a comparable component on a Microsoft Windows OS (see Appendix D: Methodology for "Reduced" Linux Desktop Configurations, for details.) I will refer to this reduced subset of ubuntu606d as ubuntu606d-reduced.

In ubuntu606d-reduced, Ubuntu issued 29 security advisories during 24 patch events addressing 85 vulnerabilities during H1 2008, so the exclusion of optional components eliminates about 38% of vulnerabilities from the analysis. 31 of the 85 were rated High severity.

Figure 13 charts the vulnerabilities, broken out by nvd.nist.gov severity, by each Patch Event in the first half of the year.

Summary

This report covered a broad set of analysis for vulnerabilities affecting Apple, Microsoft, Red Hat and Ubuntu during the first half of 2008.

Combined, the vendors fixed 585 vulnerabilities in 1H08. As context, this number measures roughly 25% of the number of new vulnerabilities disclosed during 1H08 across the industry¹⁵. Of the 585, 26.8% affected multiple vendors and of those, only 8 were fixed on the same day – the rest had an average 35 day delay between the first available fix and the last available fix..

At the individual vendor level, Red Hat fixed the most issues (292) across all of the products they support and Microsoft fixed the fewest issues (58). In an effort to minimize the perceptive impact of lower severity issues, I applied a weighting system based upon severity ratings – dividing Medium severity issue by 5 and Low severity issues by 20. The weighted analysis still had Red Hat at the top, but it was at a greatly reduced weighted value of 121.5. In contrast, Microsoft's weighted value decreased only a small amount to 53.2.

We also examined the average Days of Risk (DoR), or how long it takes a vendor to patch an issue after it is publicly disclosed. Microsoft provided fixes with the least DoR, on average, at 24.2 days. Ubuntu has the next lowest average at 72 days, followed by Apple at 98 days and Red Hat at 105. Again, I applied the weighting for severities and the order changed to these weighted values: Microsoft (25), Ubuntu (51), Red Hat (63), and Apple (82). Note that this change shows that Red Hat in particular tend to fix their higher severity issues much quicker, relative to their lower severity issues. Apple, in contrast, did not change as much in the weighted values, indicating that some of the higher severity issues are driving their DoR averages.

Another interesting number was how many issues were fixed within one day of public disclosure. Roughly 90% of Microsoft issues were fixed within a day of public disclosure – relatively good news for Microsoft customers. I believe this high number reflects some level of success at promoting responsible disclosure within the researcher community. For the other vendors, a contributing factor to their lower numbers may be inherent to the open source model – many different products and distributions share the same code. We saw this in 1H08 in the fact that 26.8% of the vulnerabilities were fixed by more than one of Apple, Red Hat and Ubuntu. Out of all of those shared vulnerabilities, only eight of them were fixed on the same day by all of the vendors examined here. For all other cases, the first fix released by a vendor acts as a public disclosure for all other affected vendors, if the issue is not yet public.

Moving on from the vendor level view, we drilled into the most recent supported enterprise desktop product for each vendor and did some work to exclude issues affecting optional Linux components that would not commonly be installed on a customer desktop. While Windows Vista users saw the fewest vulnerabilities in 1H08 at 21, Windows XP SP2 users had cause for celebration as well. With 26 vulnerabilities fixed in 1H08, Windows XP experienced a 25% reduction from the previous year. After excluding optional (and uncommon) components from the Linux distributions, Ubuntu606d-reduced was next lowest with 85 vulnerabilities, followed by rheld5c-reduced with 106 and Mac OS X 10.5 with the most at 138 vulnerabilities. We again applied a weighted analysis and the product order stayed the same.

¹⁵ See Microsoft Security Intelligence Report, <http://www.microsoft.com/sir>.

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, and provides several vulnerability-related metrics 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 these vulnerability 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, do you experience more risk on a system that has 10 vulnerabilities in a year or one that has 100 vulnerabilities in a year?

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?

All other things being equal, would you rather have a vendor that consistently provided fixes for publicly disclosed vulnerabilities in 30 days or in 120 days?

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. All other things being equal, faster patches from the vendor enable me to reduce exposure.

Also, for clarity, here are some basic definitions and assumptions as used in this report.

Vulnerabilities. *Vulnerabilities* are weaknesses in software that allow an attacker to compromise the integrity, availability, or confidentiality of that software. Some of the worst vulnerabilities allow attackers to run arbitrary code on the compromised system.

Severity scores used in this report are those scores published by the National Institute of Standards (NIST) in the National Vulnerability Database (NVD) (<http://nvd.nist.gov>).

Patch Events. I refer to those “days when at least one update is released” as a Patch Event. Looking at the number and frequency of Patch Events doesn’t reflect on the security quality of the code, but it is likely of interest to security team that gathers when an update is released to assess applicability and decide on the deployment strategy.

Days of Risk. Days of risk (DoR) is a metric that I believe is best measured at the vendor level across multiple products, since it is aimed at measuring how the combination of vendor policy, resources and decision making combine to enable a vendor to provide a fix to address a publicly disclosed vulnerability.

Publicly disclosed, in the context of this report, means broadly known to a potentially large set of attackers due to discussion in a publicly available document or web site – typically Bugtraq, a bugzilla site, or similar. The public disclosure of a vulnerability greatly increases the pool of potential attackers that could develop exploits against target customers.

Briefly, a few words on what the DoR calculations in this report are and are not and the assumptions made in calculations:

DoR is measured as the time from public disclosure until a vendor fix is available, a time of increased risk for customers.

DoR calculations here do not consider possible non-patch mitigations.

DoR here is not equivalent to a “time to fix” measure for the vendor, which would measure the time from vendor notification until a fix is available.

Though DoR is calculated for vulnerabilities fixed in H1 2008, if the public disclosure was prior to the start of the period, the full DoR window starts at the public disclosure date.

If a vulnerability affects more than one product, but the vendor provides a fix for all products on the same day, that is counted as a single DoR window.

If vulnerability affects more than one product and the vendor provides fixes for different product on different days, each fix is counted as a separate DoR window and averaged.

If a vulnerability is public before a product was generally available, the DoR window starts on the product availability date (no risk possible before the product was available).

If a vulnerability affects multiple versions of a product and they are all fixed on the same day, it is treated as one DoR window for the oldest version of the product. (It does not get averaged down just because additional versions shipped later.)

Appendix B: Terms and Abbreviations

As is common in the industry, this report uses acronyms and abbreviations quite a bit. To make things easier, I will go ahead and define some of the more common ones I use throughout the report.

- NIST. National Institute of Standards and Technology. NIST is a non-regulatory federal agency within the [U.S. Department of Commerce](#) with the mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
- NVD. National Vulnerability Database. The NVD is the U.S. government repository of standards based vulnerability management data maintained and published by NIST at <http://nvd.nist.gov>.
- CVE. Common Vulnerabilities and Exposures. The CVE list is a dictionary of publicly known information security vulnerabilities and exposures, developed and maintained by the Mitre Corporation at <http://cve.mitre.org>. Vulnerabilities can be uniquely named using their *CVE Identifier*.
- CVE Identifier. A unique vulnerability name of the format CVE-YYYY-NNNN, where YYYY is the year the identifier was assigned in the CVE List (not necessarily when discovered or disclosed).

Appendix C: 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
- Apple Security Updates as published at <http://support.apple.com/kb/HT1222>.
- Red Hat Security Advisories as published at <https://rhn.redhat.com/errata>, as well as data from <http://www.redhat.com/security/data/metrics/>.
- Ubuntu Security Notices as published at <http://www.ubuntu.com/usn>.

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.

Appendix D: Methodology for “Reduced” Linux Desktop Configurations

It has been asserted that comparing Windows to Linux distributions is like comparing “apples to oranges”, due to the fact that a Linux distro has many optional stack application components not available in Windows. At the end of the day, with products that are reasonable market alternatives to each other, there must be a reasonable method for comparison that reflects aspects of what the customer experience will be.

For example, RHEL 5 ships with Apache, MySQL and many other “server” applications. However, it is also worth noting that Linux distro vendors typically design their desktop software installer to exclude those components from the default installation and a typical desktop user would not have them installed.

To account for the differences and enable a more “apples to apples” comparison, for both Red Hat and the Ubuntu products, I install using the desktop installation defaults (which excludes most of the optional packages) and additionally

- excluded “Office” packages (e.g. OpenOffice, Evolution, Thunderbird), since Microsoft Office is not included with the Windows client operating systems
- excluded “Graphics” packages (e.g. Gimp, ImageMagick), since Microsoft Expression products are not included with Windows client operating systems

Note that this process means that Apache, MySQL and all of those optional “server” components are not installed either. After installation, I use the appropriate package management tool (i.e., rpm or dpkg) to list out the actual packages installed and use that to filter on affected components and don’t count vulnerabilities in any of the components that aren’t installed.

I would like to note that Windows Vista and Windows XP have different components too. Windows Vista Ultimate includes Media Center for example, which was not in Windows XP Professional. Similarly, both Windows XP and Windows Vista ship with version of Internet Information Server (IIS) and if those components have vulnerabilities I *will* count them against Windows, even though I don’t count Apache issues against the Linux distributions.

No two OSes or even versions of the same OS will ever be completely “apples to apples”. However, that does not have to mean that the systems cannot be compared. Whichever OS is chosen, I believe most people will install the default set of components and use that. If vulnerabilities are in those components, they will be exposed and need to take mitigating action.