Secunia
Stay Secure

Secunia Half Year Report 2010

Letter from the CEO - An Alarming Trend for End-Users

I would like to welcome you to the first release of the Secunia Half Year Report. In this report we look at the evolution of the security threat posed by vulnerabilities over the last five years, and provide an outlook for 2010 based on the data of the first six months of this year.

The overall conclusion is that despite considerable security investments, the software industry at large still proves unable to produce software with substantially less vulnerabilities, highlighting the continued need for Vulnerability Intelligence and Patch Management.

Further, the report shows an alarming development in 3rd party program vulnerabilities, representing an increasing threat to both users and business, which, however, continues to be greatly ignored. This trend is supported by the fact that users and businesses still perceive the operating system and Microsoft products to be the primary attack vector, largely ignoring 3rd party programs, and finding the actions to secure these too complex and time-consuming. Ultimately this leads to incomplete patch levels of the 3rd party programs, representing rewarding and effective targets for criminals.

Key highlights of the Secunia Half Year Report 2010:

- Since 2005, no significant up-, or downward trend in the total number of vulnerabilities in the more than 29,000 products covered by Secunia Vulnerability Intelligence was observed.
- A group of ten vendors, including Microsoft, Apple, Oracle, IBM, Adobe, and Cisco, account on average for 38 percent of all vulnerabilities disclosed per year.
- In the two years from 2007 to 2009, the number of vulnerabilities affecting a typical end-user PC almost doubled from 220 to 420, and based on the data of the first six months of 2010, the number is expected to almost double again in 2010 to 760.
- During the first six months of 2010, 380 vulnerabilities or 89% of the figures for all of 2009 has already been reached.
- A typical end-user PC with 50 programs installed had 3.5 times more vulnerabilities in the 24 3rd party programs installed than in the 26 Microsoft programs installed. It is expected that this ratio will increase to 4.4 in 2010.

In order to aid in the development of further protection mechanisms against the vulnerability threat, Secunia is currently testing a technology, which can update a broad variety of programs from a number of different vendors. This technology will be incorporated into the Secunia Personal Software Inspector (PSI) 2.0, which is currently undergoing a technology preview, and it is our intention that Secunia PSI with Auto Updating will significantly improve the security of home users' PCs.

The Technology Preview and Beta stage is expected to take another 4-5 months, followed by the final release in late 2010. Vendors who are interested in securing end-users PCs are most welcome to contact Secunia for more information.

I hope you enjoying reading the report, and find the observations and conclusions useful.

Patch and Stay Secure,

Niels Henrik Rasmussen
CEO and Founder

Table of Contents

Secunia Vulnerability Intelligence

We first provide insight into the last five years of the security ecosystems' development with respect to vulnerabilities in software. Tracking vulnerabilities and the state of software security since 2002, the Secunia Vulnerability Intelligence database contains information about more than 29,000 products and 4,000 vendors; a valuable data-set to follow and assess the evolution of software security in an increasingly networked environment. Secunia validates, verifies, and tests the vulnerability information gathered with consistent and standard processes, which we have continuously refined over the years.

Besides the number of vulnerabilities in a specific group of programs we also look at the evolution and the distribution of important vulnerability aspects, such as the criticality, the impact, the attack vector, and the availability of patches.

Vulnerability statistics covering all products are valuable to assess the state and the evolution of software, and the security ecosystem as a whole. On the other hand, looking at a specific portfolio of products provides insight into the risk exposure for users of the respective products. In the first part of the report we look at the global picture covering all vulnerabilities in all products, followed by the analysis of vulnerabilities affecting the products and the operating system found on typical end-users PCs.

Secunia Advisories

Whenever a new vulnerability is reported, Secunia releases a Secunia Advisory after verifying the information. A Secunia Advisory provides a number of details on the vulnerability, thereby providing the information needed to make appropriate decisions about how to protect systems. The details include a description of the vulnerability, risk rating, impact, attack vector, recommended mitigation, credits, and references. After the first publication, Secunia tracks the status of the vulnerability throughout its lifecycle and updates the corresponding Secunia Advisory as new relevant information becomes available. For example, when a vendor releases a patch for a vulnerable product, the status of the Security Advisory is changed to "patched". Generally, Secunia releases, or updates, a Secunia Advisory when new information becomes available. This enables the administrator of the vulnerable software to take appropriate action when needed. In case several vulnerabilities are released at the same time (if these vulnerabilities affect the same product and result in one administrative action) these will be reported in one Secunia Advisory. Likewise several Secunia Advisories are released for a vulnerability affecting different products and requiring different administrative actions. Secunia generally does not report vulnerabilities in beta-versions of programs.

For all products in the Secunia vulnerability database the left panel of Figure 1 shows the number of Secunia Advisories released in a given year since 2005. On average Secunia released 3,422 Secunia Advisories per year from 2005 to 2009 with a standard deviation of 400 Secunia Advisories (12% of the average). An extrapolation of the data from the first half of this year indicates an increased number of Secunia Advisories for 2010 compared to the previous years. For this analysis we excluded "update for" Secunia Advisories for Linux distributions as these all are duplicates of already disclosed vulnerabilities.

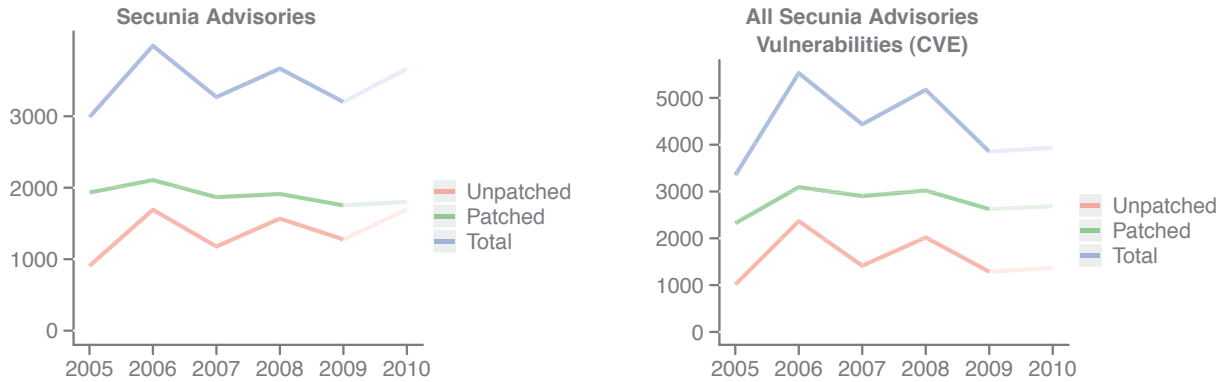

Figure 1 Number of Secunia Advisories and vulnerabilities Common Vulnerabilities and Exposures (CVE) together with the solution status since 2005. The plots include a linear extrapolation for 2010 based on the data of the first half of 2010.

Vulnerabilities

Common Vulnerabilities and Exposures (CVE)[1] is a de facto industry standard to uniquely identify vulnerabilities which has achieved wide acceptance in the security industry. Using CVEs as vulnerability identifiers enables the correlation of information about vulnerabilities between different security products and services. Secunia assigns CVE information in Secunia Advisories. If CVE information becomes available after the release of a Secunia Advisory, it will be updated. The right panel of Figure 1 shows the number of CVEs disclosed per year since 2005 with a break-down of the solution status ("unpatched", "patched", "total"). On average Secunia reported 4,464 CVEs per year in the Secunia Advisories from 2005 to 2009 with a standard deviation of 904 CVEs (20% of the average). We observe more volatility in the number of CVEs than in the number of Secunia Advisories per year. An extrapolation of the data of the first half of 2010 lets us expect 2010 to exceed the number of CVEs of 2009, but not the average of the last five years. It should be noted that older vulnerabilities are more likely to have a patch available than recently found vulnerabilities. Therefore, the number (and the extrapolation) of unpatched CVEs typically show an increase in the last year of the observation period. This increase should not be mistaken as a general trend towards decreased security, but as an artifact of the recency of the data.

The Secunia Advisory count is a first order approximation for the number of Vulnerability Events, which is the number of administrative actions required to keep the specific product secure throughout a given period of time.

Vulnerability/CVE counts are a viable metric for the number of distinct vulnerabilities found in software.

While the number of Secunia Advisories estimates vulnerability events (the number of administrative actions needed to assess or maintain software), the number of CVEs can be used as an approximation for the number of unique vulnerabilities affecting the products observed.

Over the last five years the total number of CVEs and Secunia Advisories fluctuates but shows no clear trend. Thus, at a large scale the security ecosystem appears to be in a state of equilibrium, at the current rate of CVEs, supporting that generally software vendors are still unable to release vulnerability free software. There is therefore a continued need for effective vulnerability management, for users and administrators of all types of software, and for software vendors in general to focus more on writing secure code.

Top-10 Vendors with the most Vulnerabilities

To gain more insight into the security ecosystem we identify the group of the ten vendors with the most vulnerabilities (in all their products) in any given year. Since 2005 these Top-10 vendors are responsible for about 38% of the total vulnerabilities representing 16% of the Secunia Advisories per year. The composition of the Top-10 group varied only slightly in this period; seven of the Top-10 vendors with the highest vulnerability counts in 2005 are still in the Top-10 group in 2010.

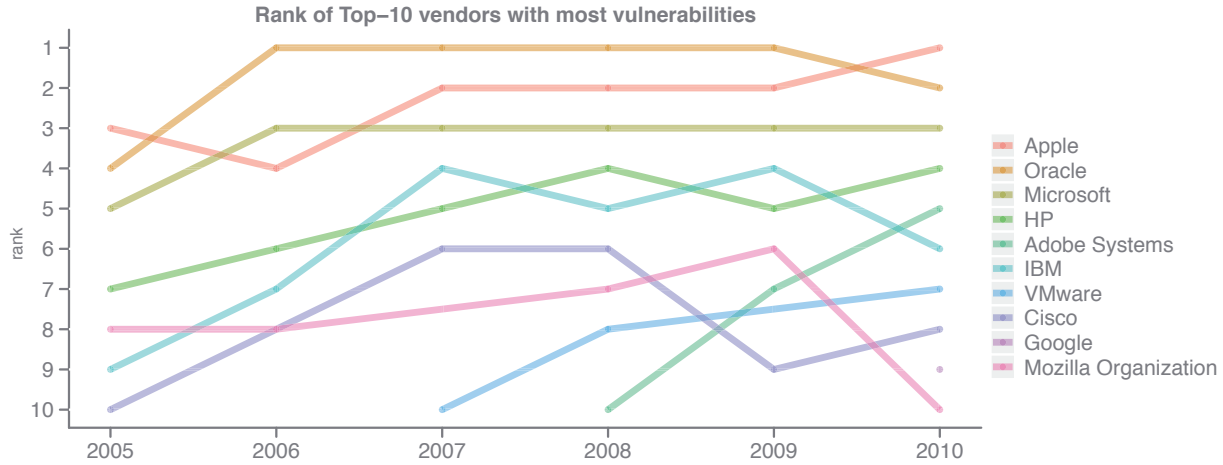

Figure 2 Ranking of the Top-10 vendors with most vulnerabilities per year. Oracle includes also vulnerabilities from Sun Microsystems and BEA logic.

[1] *Common Vulnerabilities and Exposures (CVE), http://cve.mitre.org*

To visualize the dynamics in the Top-10 group we first identify the ten vendors with the most vulnerabilities in 2010 (up to June) and then plot the rank of each of these vendors for the previous five years. The result is visualized in Figure 2. The above graph is not an indication of the individual vendors' security, as it is not possible to compare the vendors based on number of vulnerabilities alone. To assess the "performance" of vendors in terms of vulnerabilities one should rather look at the changes in the type of vulnerabilities, code quality, handling of vulnerability reports, ability to update users, quality of patches, ability to communicate to end users, number of products, complexity of product portfolio, and other factors which cannot be read out of mere aggregate numbers.

Figure 2 visualizes the dynamics in the Top-10 group and indicates that popular vendors are also subject to more scrutiny by the security community/researchers than less popular vendors; Oracle (including Sun Microsystems and BEA Logic) ranked #1 in four out of five years overtaken by Apple in the first half of 2010, with Apple consistently ranking higher than Microsoft. Despite increased investments into the security of their products, none of the seven vendors who occupied the Top-10 group in 2005 as well as in 2010 managed to decrease the number of vulnerabilities discovered in their products. On the contrary, the vulnerability count of each of these seven vendors has increased to reach in 2009 between 136% and 440% of the 2005 count.

This analysis also supports the general perception that a high market share correlates with a high number of vulnerabilities. Apple (iTunes, Quicktime), Microsoft (Windows, Internet Explorer), and Sun Microsystems (Java, now part of Oracle) consistently occupy the top ranks during the last five years, with Adobe (Acrobat Reader, Flash) joining the group in 2008. The ranking shown in Figure 2 does not indicate the actual security (or lack thereof) in the different vendors products; it rather shows that vulnerabilities continue to be discovered in significant numbers in products from even the largest and most popular vendors including those who spend significant resources on improving the security of their products.

> On average, **10 vendors** are responsible for **38%** of the vulnerabilities per year.

Attack Vector

The attack vector describes the way an attacker can trigger or reach the vulnerability in a product. Secunia classifies the attack vector as either "Local system", "Local network", or "From remote". The classification of the three attack vectors together with a description of how they are used in Secunia Advisories is listed in the Appendix of this report. Figure 3 plots a breakdown by attack vector as a percentage of the total number of Secunia Advisories by year. We observe that "From remote" is consistently and by far the most prevalent attack vector (81% in average), compared to "Local system" with 9.8% and "Local network" with 8.2% in average over the last five years. Thus, most of the vulnerabilities expose the user of the software to remote attacks. Based on the data available by mid 2010 we do not expect a change by the end of the year.

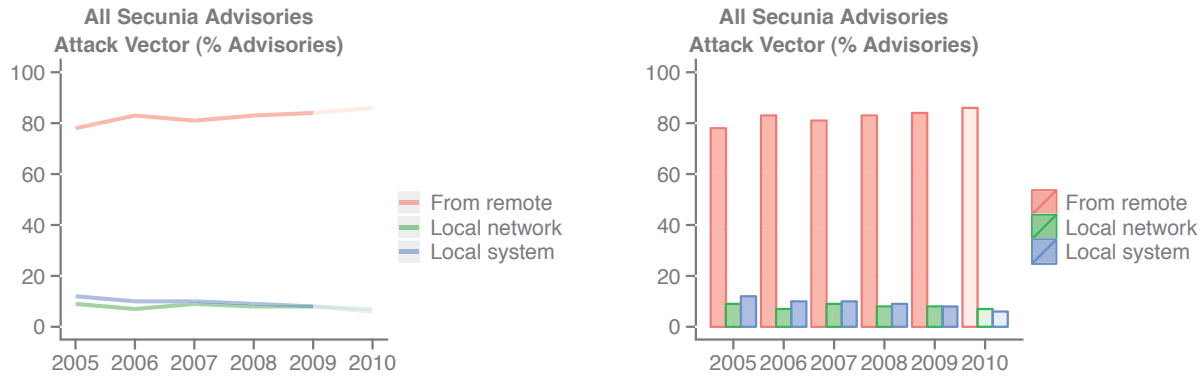

Figure 3 Percentage of Secunia Advisories per year for each attack vector from 2005 to 2009, with a linear extrapolation for 2010.

Criticality

Secunia rates the criticality of vulnerabilities on a five level criticality scale, ranging from "Not critical" to "Extremely critical". The criticality of a vulnerability is based on Secunia's assessment of the vulnerability's potential impact on a system, the attack vector, mitigating factors, and if an exploit exists for the vulnerability prior to release of a patch. In the Appendix of this report we list the criticality classification together with a description of how they are used to rate the risk of a vulnerability. Figure 4 shows that from 2005 to 2009 more than 50% of the vulnerabilities were rated highly or moderately critical, while 33% were rated less critical, and only very few as extremely critical (0.2%). The distribution of the risk ratings has not changed substantially over the last years, and it clearly depends on the mix of products being looked at. Figure 4 analyzes the criticality distribution over all products. The same methodology can be applied to a specific group of products to provide an accurate picture of the risk profile due to vulnerabilities in these products.

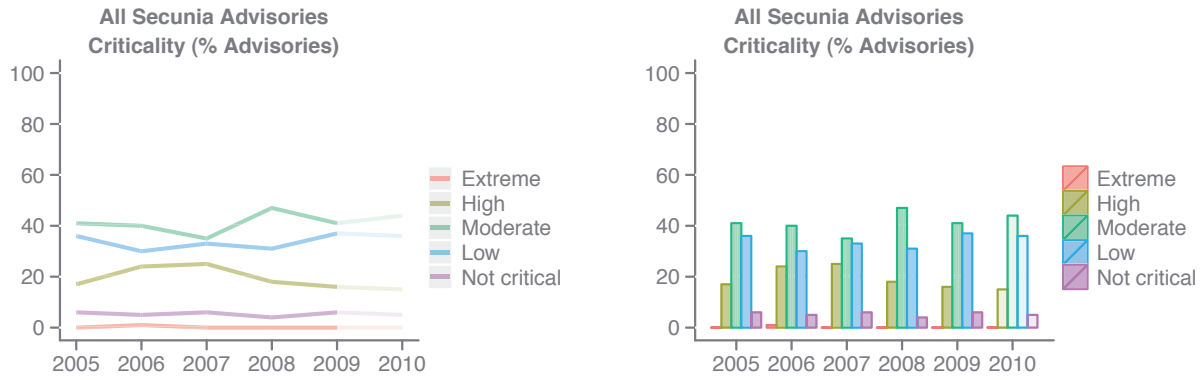

Figure 4 Risk classification as percentage of all vulnerabilities in all products per year from 2005 to 2009, with a linear extrapolation for 2010.

Impact

Secunia tracks and classifies the impact of successful exploitation of a given vulnerability on the affected system. The impact classification ranges from consequences such as "Exposure of system information" to "System access" and is listed in the Appendix of this report. As with the criticality rating, the impact rating depends considerably on the type or mix of software looked at. In Figure 5 we plot the percentage of the six most prevalent impact classes since 2005. Throughout the last five years the most prevalent impact class is "System access" with an average of 33%. System access allows an attacker to execute arbitrary code or commands from remote.

Figure 5 Distribution and evolution of the six most prevalent impact classes since 2005. The plots include a linear extrapolation for 2010 based on the data of the first half of 2010.

Security of End-User PCs

In the previous section we looked at all vulnerabilities. However, to get a better understanding of the risk that most Internet users face, we now focus our analysis on products typically found on end-user PCs, and consider only vulnerabilities found in these products.

The variety and prevalence of programs found on typical end-user PCs, paired with the unpredictable usage patterns of users, makes end-user PCs an attractive attack vector.

Vulnerabilities on end-user PCs are commonly exploited when the user of the vulnerable computer visits a malicious Web site (with content controlled or injected by an attacker), or opens data, files, or documents, with one of the numerous programs and plug-ins installed on his/her PC. Recent research revealed that typically 50% of the users are found to have more than 66 programs from more than 22 different vendors installed[2]. To assess the associated risk we identify the Top-50 most prevalent programs on typical end-user PCs based on empirical data from users frequently scanning their PCs with Secunia Personal Software Inspector (PSI)[3].

Secunia PSI is a free security tool designed to detect vulnerable and out-dated programs and plug-ins which expose your PC to attacks. Since 2007 more than **2.5 million users** installed Secunia PSI to help protect their PCs

The Top-50 Software Portfolio comprises the 50 most prevalent programs found on typical end-user systems. It consists of 26 Microsoft and 24 non-Microsoft (3rd party) programs from a total of 14 different vendors (including Microsoft).

Typically, 50% of the users are found to have more than 66 programs from more than 22 different vendors installed.

Secunia PSI is a free program to check all programs found on a system for missing security related patches, and old versions (end-of-life programs). Secunia PSI works by examining files on the user's PC (primarily .exe, .dll, and .ocx files). After examining all relevant files on local hard drive(s), the collected data is matched against Secunia's file signatures engine to determine the exact version of the programs installed. Secunia PSI data provides accurate information on the installation base of the users' PC - that is, the user's software portfolio. We identified the group of the Top-50 most prevalent programs by looking at all PSI scans in May 2010. This group represents a typical users' software portfolio and contains programs from 14 different vendors, of which 26 programs are from Microsoft and 24 programs from 3rd party vendors. The user share of the most prevalent program in this Top-50 group is equal to 100% (Microsoft Internet Explorer), whereas the share of the least prevalent program in this group is 24% (PowerDVD from Cyberlink). Thus, the Top-50 group only contains programs with a market share of at least a 24% across all PSI users supporting the relevance of the choice of the Top-50 programs.

2 *Secunia Paper: "The Security Exposure of Software Portfolios" http://secunia.com/gfx/pdf/Secunia_RSA_Software_Portfolio_Security_Exposure.pdf*

3 *Secunia PSI, http://secunia.com/vulnerability_scanning/personal*

Typical Software Portfolio & Operating System

We first examine the number of vulnerabilities of this Top-50 software portfolio together with the operating system, namely Windows XP and Windows Vista. Windows 7, released in October 2009, is excluded as we have no full year of data yet. In Figure 6 we plot the combined number of vulnerabilities of the Top-50 portfolio including the vulnerabilities of the operating system Windows XP. Accordingly, Figure 7 shows the Top-50 portfolio together with Windows Vista.

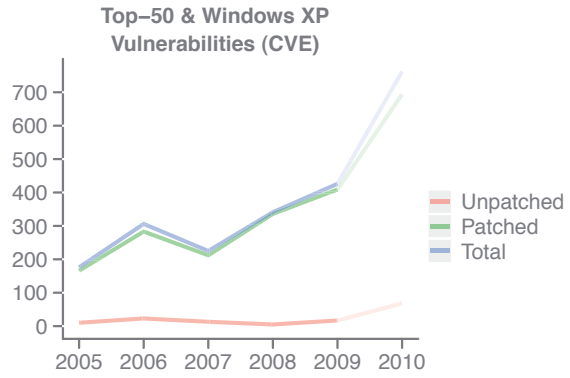

Figure 6 Vulnerabilities per year of Windows XP including the Top-50 most prevalent programs.

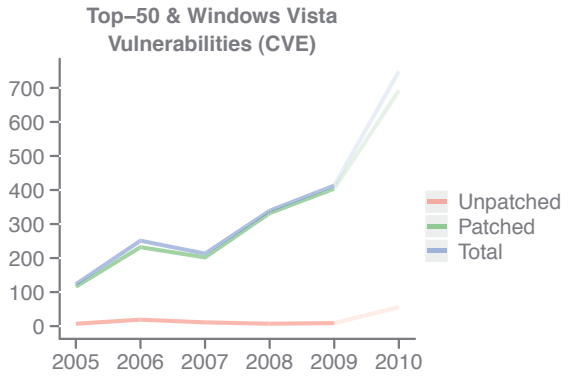

Figure 7 Vulnerabilities per year of Windows Vista including the Top-50 most prevalent programs. Before 2007 this plot only shows Top-50 vulnerabilities as Windows Vista was released in the end of 2006

Since 2007 the combined number of vulnerabilities (Top-50 portfolio and operating system) increased progressively from about 220 and almost doubled to 420 by 2009. During the first 6 months of 2010 we already reached 380 vulnerabilities, or 89% of the figures for the entire 2009. If we extrapolate the number of vulnerabilities discovered in the 1st half of 2010 for the 2nd half we will reach approximately 760 vulnerabilities for the whole of 2010.

Looking at a typical end-users Top-50 software portfolio we find that the choice of operating system only has a marginal affect on the total number of vulnerabilities the user is exposed to (a difference of less than 2% since 2008). Despite the small difference in the aggregate number of vulnerabilities for the software portfolio due to the operating system, it is important to remember that Windows Vista and Windows 7 offer many security features not present in Windows XP[4]. In Figure 8 we analyze the criticality of the vulnerabilities of the Top-50 portfolio together with the respective operating system. We find that on average 50% of Secunia Advisories are rated as highly critical, and 7.6% are rated as extremely critical, whereas in Figure 4 (covering all products) we only find an average of 0.2% extremely critical Secunia Advisories. This supports the trend towards the increased security threat facing the typical users. The observed continued increase in the number of vulnerabilities of a typical user PC, paired with the high criticality rating of most vulnerabilities, indicates a substantial increase of the end-users risk since 2007.

Top-50 programs & OS

From 2007 to 2009 vulnerabilities in a typical end-user PC **almost doubled** from about **220** to **420**.

If we **extrapolate** the number of vulnerabilities discovered in the 1st half of 2010 for the 2nd half we will reach in the neighborhood of **760 vulnerabilities** in 2010.

During the first 6 months of 2010 we already reached **380** vulnerabilities or **89%** of the figures for the entire 2009.

4 *Secunia Paper: "DEP/ASLR Implementation Progress in Popular Third-party Windows Applications" http://secunia.com/gfx/pdf/DEP_ASLR_2010_paper.pdf*

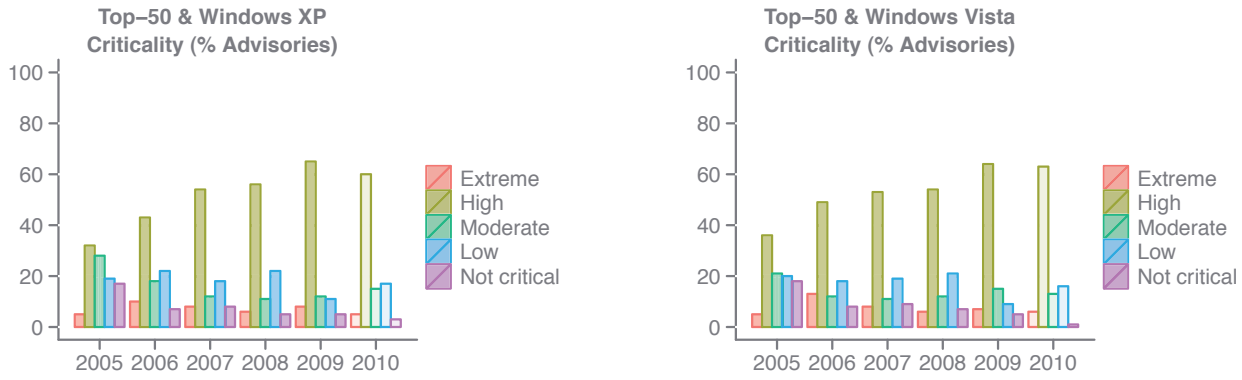

Figure 8 Criticality rating of the Top-50 portfolio with Windows XP (left) and Windows Vista (right)

Software deployed requires constant attention due to the continued discovery of new vulnerabilities and release of patches. Upon the disclosure of a vulnerability, or the release of a patch, the administrator (or user) must assess the risk involved, and in the case of a patch plan and schedule its deployment. In order to estimate the attention needed to keep specific products up-to-date we use the number of Secunia Advisories as an approximation for the number of vulnerability events in a given period of time. Vulnerability events per year are provided in Table 1 (see Page 12).

Contribution of 3rd Party Programs

Interestingly, since 2005 we find a significant rise in the number of vulnerabilities of the Top-50 software portfolio while no trend is identified in the global vulnerability data presented in Figure 1. To better understand the dynamics in the Top-50 portfolio we plot a breakdown of the Top-50 portfolio by vulnerability contributions from (A) the Operating System, (B) Microsoft programs, and (C) from 3rd party (non-Microsoft) programs. In Figure 9 we show the result for Windows XP (left) and Windows Vista (right). This analysis clearly identifies vulnerabilities from 3rd party programs to be almost exclusively responsible for the increasing trend observed since 2007. Data from the first half of 2010 shows that 3rd party program vulnerabilities are the primary risk factor for typical end-user PCs.

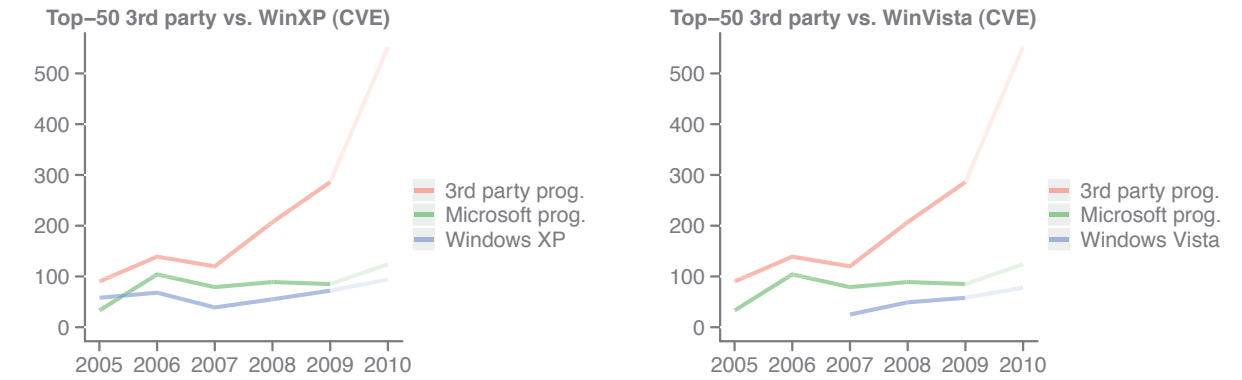

Figure 9 Breakdown of the Top-50 portfolio vulnerabilities into Operating System, Microsoft-, and 3rd party (not from Microsoft) programs.

Selected values from Figure 9 together with the number of vulnerability events are summarized in Table 1. A detailed view is given in Table 2 with a breakdown by operating system and both Microsoft and 3rd party programs of the Top-50 software portfolio.

Vulnerabilities (unique CVEs)					
	2007	2008	2009	YTD 2010	trend 2010
Top-50 & Windows XP	225	341	426	380	760
Top-50 & Windows Vista	213	339	413	373	746

Vulnerability Events (Secunia Advisories)					
	2007	2008	2009	YTD 2010	trend 2010
Top-50 & Windows XP	106	107	110	75	150
Top-50 & Windows Vista	95	105	104	67	134

Table 1 Selected values from Figure 6 and Figure 7 together with the number of vulnerability events, including 2010 year-to-date (YTD) value and the trend to end of the year

Vulnerabilities - Breakdown					
	2007	2008	2009	YTD 2010	trend 2010
Windows XP	39	55	72	47	94
Windows Vista	25	49	58	39	78
Microsoft programs	79	89	85	62	124
3rd party programs	120	207	286	275	550

Vulnerability Events - Breakdown					
	2007	2008	2009	YTD 2010	trend 2010
Windows XP	31	33	35	27	54
Windows Vista	18	30	28	19	38
Microsoft programs	40	35	27	18	36
3rd party programs	43	42	51	32	64

Table 2 Number of vulnerabilities and vulnerability events from Table 1 including breakdown by operating system, Microsoft and 3rd party programs.

Why 3rd Party Programs?

In recent years there has been an increased focus on 3rd party programs by vulnerability researchers and by criminals. In our opinion this is a natural development; a decade ago the primary focus for research and exploitation was in services, especially typical Internet facing services, this changed to include services that ideally should not be exposed to the Internet, such as Windows file sharing. However, as vendors started to take notice of the cyber risks, and administrators learned that firewalls (personal as well as perimeter firewalls) were necessary to filter out the most obvious unwanted traffic, we also saw a change in focus from both researchers and criminals towards the most popular products from Microsoft, ranging from the operating system, to the browser, and office products. In response to this, Microsoft has enabled most users and even businesses to update their PCs with patches in a timely manner; pushing and enabling Windows Update and promoting Windows Service Update Services (WSUS) to businesses for free. This has lead to a very small "window of opportunity" for criminals to actively exploit vulnerabilities in Microsoft products, because many users are updated fairly rapidly.

Today we are facing a much more challenging and complicated problem that is likely to take years to solve; patching of 3rd party software. Looking at the Top-50 programs installed by Secunia PSI users we see that the programs come from 14 different vendors, it is also worth considering that all the programs covered by Secunia PSI is spanning a total of 3,000 vendors. Only recently have we seen significant initiatives from Adobe, the most prevalent "3rd party" vendor due to Adobe Flash Player and Adobe Reader, to start updating all their users in a more efficient and rapid manner than earlier. This seems to be a response to the increased exploitation of Adobe Reader vulnerabilities in 2009.

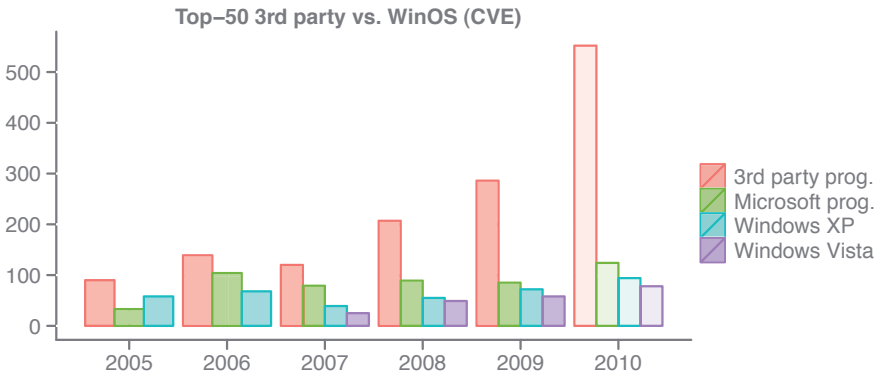

Figure 10 Breakdown of the Top-50 portfolio vulnerabilities into contributions from 3rd party (not from Microsoft) programs, Microsoft programs and the operating system (Windows XP or Windows Vista).

The number of vendors who are deploying and promoting effective updating mechanisms is quite limited, it includes Microsoft, Google, Mozilla Foundation, Adobe, and possibly a few more, but the overall picture of all vendors, including most of the more popular vendors, is that updating of the programs on end-user PCs is largely neglected and left to the end-user.

It appears that most vendors do not take significant steps to secure their users and customers before active exploitation takes place on a larger scale where it starts to threaten the overall reputation of the business. The lack of effective updating mechanisms expose end-users to significant risks as vulnerable software tends to "survive" for a long time before being updated for other reasons than security, thus leaving the user exposed for prolonged periods of time and providing criminals ample time to exploit the vulnerabilities.[5]

Further, the typical users are either unaware, or simply overwhelmed by the complexity and frequency of the actions required to keep the dozens of 3rd party programs found on a typical end-user system secure. To keep the Top-50 software portfolio fully patched the user can patch the operating system and 26 Microsoft programs with one easy to use auto-update mechanism. To patch the remaining 24 3rd party programs from 13 different vendors typically requires managing another 13 or more different update mechanisms.

In other words, the user has one auto-update mechanism to patch 48% of the programs that make up 35% of the vulnerabilities in 2009 and another 13 or more update mechanisms to patch 52% of the programs that make up 65% of the vulnerabilities.

It is therefore a safe guess that users will hardly update all their 3rd party programs in a timely fashion, supported by the overall reasons of:

- User's and businesses alike still perceive the operating system and Microsoft products to be the primary attack vector, largely ignoring 3rd party programs.
- Many 3rd party programs lack a noteworthy and easy to use update mechanism.
- The frequency and complexity of managing a large number of different update mechanisms will almost certainly lead to incomplete patch levels at large.
- General lack of awareness among users and professionals about the consequences of having vulnerable programs installed.

From an attacker's perspective, targeting 3rd party programs proves to be a rewarding path, and will probably remain so for an extended period of time. Few vendors like Microsoft have the financial resources and expertise to consistently make the exploitation of their software harder, and to implement a

Typically, a user can patch **35%** of the vulnerabilities with **one** update mechanism (Microsoft's), and needs to master another **13 or more different** update-mechanisms to patch **65%** of the 3rd party program vulnerabilities.

5 *Paper: "Why Silent Updates Boost Security" http://www.techzoom.net/papers/browser_silent_updates_2009.pdf*

formidable "seamless" and easy to use auto-update mechanism to effectively relieve the users from the complexities of keeping their software up-to-date. Further, as the number of vulnerability events and the complexity of the task increase, cyber-criminals are provided a larger number of unpatched targets.

Therefore, focusing on 3rd party program exploitation will continue to provide attackers with a large pool of commonly used software that is easier to exploit[6], and much less likely to be found fully patched.

Top-10 3rd Party Programs (ranked by # of vulnerabilities)				
			June 2009-2010	
Rank Program	**Vendor**	**Installation share**	**CVEs**	**Events**
1. Mozilla Firefox	Mozilla Foundation	56%	96	15
2. Apple Safari	Apple	15%	84	9
3. Sun Java JRE	Sun (Oracle)	89%	70	5
4. Google Chrome	Adobe	30%	70	14
5. Adobe Reader	Adobe	91%	69	7
6. Adobe Acrobat	Adobe	8%	69	7
7. Adobe Flash Player	Adobe	99%	51	4
8. Adobe AIR	Adobe	41%	51	4
9. Apple iTunes	Apple	43%	48	3
10. Mozilla Thunderbird	Mozilla Foundation	10%	36	7

Table 3 List of the Top-10 non-Microsoft programs with the most vulnerabilities in the 12 month from June 2009 to June 2010. Source: Secunia PSI.

Top-10 Microsoft Programs (ranked by # of vulnerabilities)				
			June 2009-2010	
Rank Program	**Vendor**	**Installation share**	**CVEs**	**Events**
1. Internet Explorer	Microsoft	100%	49	12
2. Excel Viewer	Microsoft	2%	37	4
3. Excel	Microsoft	78%	30	5
4. Visual Studio	Microsoft	5%	15	3
5. .NET Framework	Microsoft	95%	13	4
6. Visio Viewer	Microsoft	35%	11	2
7. Visio	Microsoft	3%	11	3
8. Word Viewer	Microsoft	3%	9	2
9. Works	Microsoft	7%	9	2
10.Project	Microsoft	3%	9	2

Table 4 List of the Top-10 Microsoft programs with the most vulnerabilities in the 12 month from June 2009 to June 2010. Source: Secunia PSI.

Table 3 shows the list of the Top-10 3rd party programs with the highest number of vulnerabilities in the last 12 months together with the number of vulnerability events during the same period. For each program listed we also show the share of PSI users found to have it installed. Accordingly, Table 4 lists the Top-10 Microsoft programs ranked by the number of vulnerabilities in the same period.

The number of vulnerabilities in a given product is not necessarily equal to the overall security of the product. It is important to consider that vendors have different policies for assigning CVEs and that the numbers doesn't reflect the rating of the vulnerabilities, the type of vulnerabilities, type of coding errors, ability to respond to the reports, and many other factors which may be relevant in a proper comparison.

6 *Secunia Paper: "DEP/ASLR Implementation Progress in Popular Third-party Windows Applications" http://secunia.com/gfx/pdf/DEP_ASLR_2010_paper.pdf*

How to reduce these Risks?

The best ways to reduce the risk we are exposed to by using software and the Internet would certainly be reducing the number of vulnerabilities and the window of opportunity to exploit vulnerabilities. Sadly, data from more than a decade shows that the industry has proved unable to reduce the number of vulnerabilities discovered in their products, and there is little hope that this will change substantially in the years ahead. By far the most effective way to reduce the risk exposure is reducing the complexity in patching the variety of programs typically found on end-user PCs. This would enable users to readily install patches and thereby reduce the window of opportunity for criminals. Two major steps towards this goal are:

- **Awareness**
  Users and businesses must change their perception that Microsoft products pose the largest threat in order to allocate security resources effectively. General awareness on the risk of 3rd party programs must be established.

- **Unified patching**
  New technology is needed to allow users to automatically install security updates for a broad array of programs.

NOTE: As a response to the lack of interest and action from the software industry in 2009[7], Secunia is currently testing technology which can update a broad variety of programs from a number of different vendors. The Technology Preview of Secunia PSI 2.0 has been available since mid-June. It is our hope that Secunia PSI with Auto Updating will significantly improve the security of home users PCs.

The Technology Preview and Beta stage is expected to take another 4-5 months, with an expected "final" release late 2010. Vendors who are interested in securing end-users PCs are most welcome to contact Secunia for more information about how Secunia can help them update their users in a "seamless" manner.

7 Patching Redefined: http://secunia.com/blog/80/

Appendix

Vulnerability Criticality Classification

Extremely Critical (5 of 5)	Typically used for remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation does not normally require any interaction and active exploitation is currently known to occur. These vulnerabilities can exist in services like FTP, HTTP, and SMTP or in certain client applications like e-mail programs and browsers.
Highly Critical (4 of 5)	Typically used for remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation does not normally require any interaction, but there are no reports of active exploitation at the time of disclosure. These vulnerabilities can exist in services like FTP, HTTP, and SMTP or in certain client applications like e-mail programs and browsers. This rating may also be used for vulnerabilities currently being exploited, but where significant user interaction is required or the attack vector is "Local network".
Moderately Critical (3 of 5)	Typically used for remotely exploitable Denial of Service (DoS) vulnerabilities against services like FTP, HTTP, and SMTP, SQL injection vulnerabilities, and for vulnerabilities that allow system compromise, but require user interaction. This rating is also used for vulnerabilities allowing system compromise on local networks in services like SMB, RPC, NFS, LPD and similar where firewall best practices recommend against making these accessible over the Internet unrestricted.
Less Critical (2 of 5)	Typically used for cross-site scripting vulnerabilities, cross-site request forgery (CSRF) vulnerabilities, privilege escalation vulnerabilities, and vulnerabilities allowing exposure of sensitive data to local users.
Not Critical (1 of 5)	Typically used for weaknesses with a very limited security impact, very limited privilege escalation vulnerabilities, and locally exploitable Denial of Service (DoS) vulnerabilities.

Table 5 Vulnerability criticality rating as used in Secunia Advisories

Attack Vector Classification

From Local System	"Local system" describes vulnerabilities where the attack vector requires that the attacker is a local, authenticated user on the system.
From Local Network	"From local network" describes vulnerabilities where the attack vector requires that an attacker is situated on the same network as a vulnerable system (not necessarily a LAN). This category also covers vulnerabilities in certain services (e.g. DHCP, RPC, administrative services) for which firewall best practices recommend that these should not be accessible from the Internet, but only from a local network or a restricted set of external systems.
From Remote	"From remote" describes vulnerabilities where the attack vector does not require access to the system or a local network. This category covers services that are acceptable to expose to the Internet according to firewall best practices (e.g. HTTP, HTTPS, SMTP). It also covers vulnerabilities in client applications where it is reasonable to assume that a security conscious user can be tricked into performing certain actions (e.g. viewing a web page or opening a file).

Table 6 Vulnerability attack vector classification used by Secunia.

Vulnerability Impact Classification

Brute force	Used in cases where an application or algorithm allows an attacker to guess passwords in an easy manner.
Cross-Site Scripting (XSS)	Cross-Site Scripting vulnerabilities allow a third party to manipulate the content or behavior of a web application in a user's browser session without compromising the underlying system. Different Cross-Site Scripting related vulnerabilities are also classified under this category, including "script insertion" and "cross-site request forgery". Cross-Site Scripting vulnerabilities are often used against specific users of a website to steal their credentials or to conduct spoofing attacks.
DoS (Denial of Service)	This includes vulnerabilities ranging from excessive resource consumption (e.g. causing a system to exhaust memory) to crashing an application or an entire system.
Exposure of sensitive information	Vulnerabilities where e.g. documents or credentials are leaked or can be revealed either locally or remotely.
Exposure of system information	Vulnerabilities where excessive information about the system (e.g. version numbers, running services, installation paths, and similar) are exposed and can be revealed from remote and in some cases locally.
Hijacking	This covers vulnerabilities where a user session or a communication channel can be taken over by other users or remote attackers.
Manipulation of data	This includes vulnerabilities where a user or a remote attacker can manipulate local data on a system, but not necessarily be able to gain escalated privileges or system access. The most frequent type of vulnerabilities with this impact are SQL-injection vulnerabilities where a malicious user or person can manipulate SQL queries.
Privilege escalation	This covers vulnerabilities where a user is able to conduct certain tasks with the privileges of other users, including administrative users.
Security Bypass	This covers vulnerabilities or security issues where malicious users or people can bypass certain security mechanisms of the application. The actual impact varies significantly depending on the design and purpose of the affected application.
Spoofing	This covers various vulnerabilities where it is possible for malicious users or people to impersonate other users or systems.
System access	This covers vulnerabilities where malicious people or malicious users are able to gain system access and execute arbitrary code with the privileges of a local system account (e.g. a specific user running a service or LocalSystem).
Unknown	Covers various weaknesses, security issues, and vulnerabilities not covered by the other impact types or where the impact is not known due to insufficient information from vendors and researchers.

Table 7 Vulnerability impact classification used by Secunia. A given vulnerability might be assigned to more than one impact class to accurately reflect its impact.

About Secunia

Secunia is the world-leading provider of Vulnerability Intelligence and Vulnerability Management tools for enterprises and the IT-Security Industry. Our solutions focus on the identification and elimination of program vulnerabilities, covering both Microsoft and 3rd party programs.

For further information please visit our website - **secunia.com**

Secunia

Weidekampsgade 14A
DK-2300 Copenhagen S
Denmark

Email: info@secunia.com
Phone: +45 7020 5144
Fax: +45 7020 5145