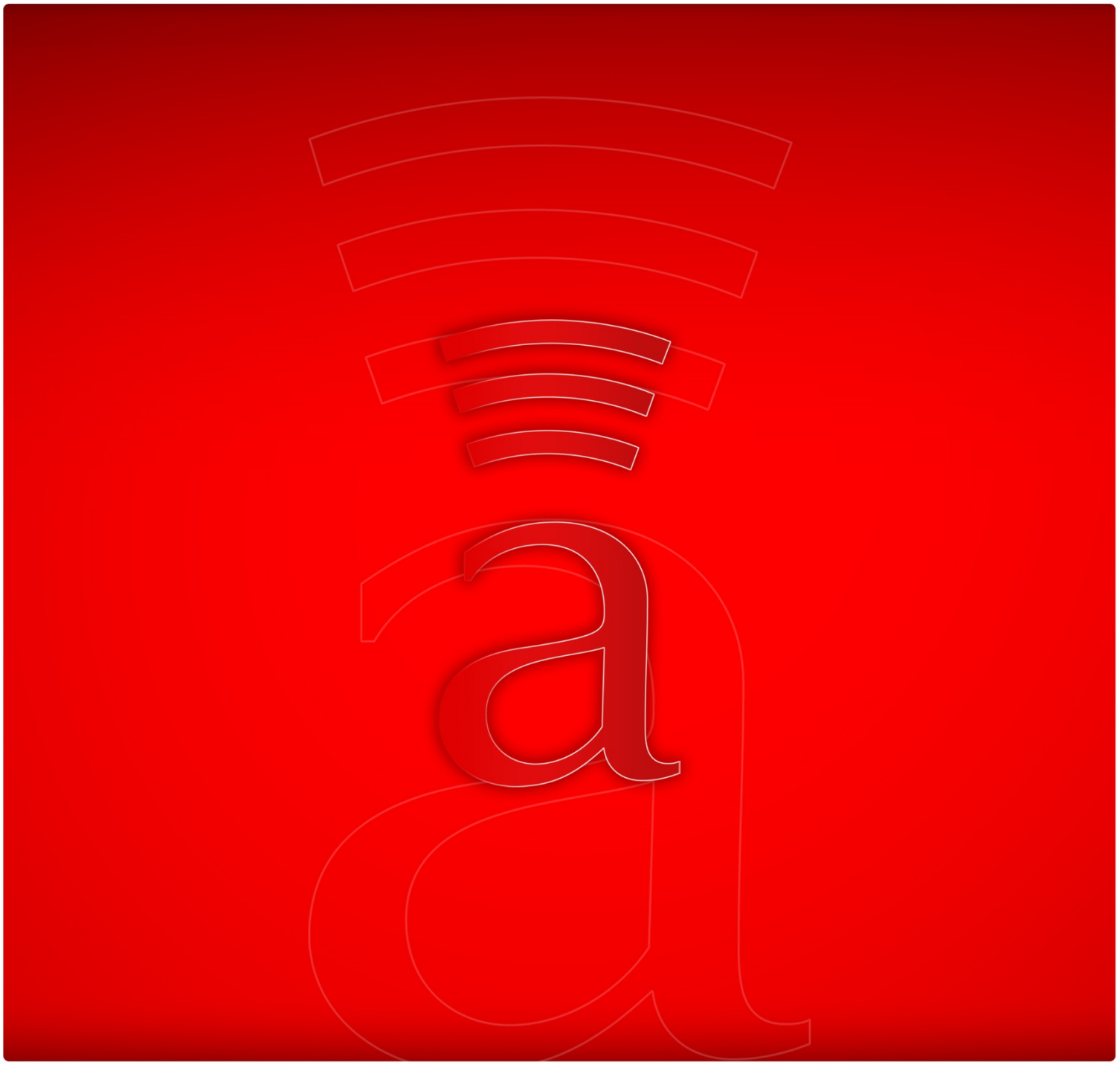
Secunia
Stay Secure

Yearly Report 2010



Abstract

This report presents global vulnerability data from the last five years and identifies trends found in 2010. The total number of vulnerabilities disclosed in 2010 shows a slight decrease of 3% compared to 2009. A significant trend, however, is revealed when looking at a representative portfolio of software typically found on end-point PCs. Vulnerabilities affecting this portfolio have increased in three years, or by 71% in the last 12 months alone. This trend is primarily the result of vulnerabilities in third-party (non-Microsoft) programs, which in turn are also much harder to patch as a result of a lack of a unifying patch mechanism. By neglecting the risk of ubiquitous third-party programs, users risk being compromised by cybercriminals every day, despite the deployment of other security measures

Table of Contents

Letter from the CEO – Reducing the Window of opportunity

I would like to welcome you to the Secunia Yearly Report 2010. In this report we move forward with the key findings and trends identified in our previous Half Year Report, to further investigate the evolution of the security threat posed by vulnerabilities over the last six months of 2010.

Looking back on the feedback we have received in 2010 from customers, end-users, strategic partners, and even competitors in mind, I am happy to conclude that we have made a leap in the right direction. We have launched Auto Updating in the Secunia PSI 2.0 and have also integrated the Secunia CSI with Microsoft WSUS and SCCM for easy patch distribution; relieving end-users and customers from the complexity and inconvenience of keeping programs up-to-date and secure.

Vulnerabilities are still the 'Achilles' Heel' of any IT system. Managing these vulnerabilities is therefore the primary means of reinforcing the strength of any IT infrastructure, thus reducing the window of opportunity for cybercriminals to exploit vulnerable programs.

However, the complexity of IT systems, lack of awareness, and more importantly, the lack of a unified and automated way to deploy critical security updates – or 'patches' – to your IT systems, results in a lengthy process. There is a huge delay from the point in time when vulnerabilities are discovered and details reach the criminals, before end-users and corporate security teams actually deploy the appropriate security updates.

Despite vulnerabilities being the weakest point in modern IT systems, all too many fail to realise the need to prioritise deployment of security updates. Even those who are aware of this often do not update in a timely fashion due to a lack of knowledge of their inventory, or simply because the security updates are difficult to deploy and other day-to-day tasks seem more urgent than the risk posed by the unpatched vulnerabilities. For example, users with the average software portfolio installed on their PCs will need to master around 14 different update mechanisms from individual vendors to update their programs and keep their IT systems protected against vulnerabilities.

For the past eight years Secunia has worked to make Vulnerability Intelligence accessible, reliable, and actionable, to help end-users and security teams understand and prioritise their efforts to remediate vulnerabilities. In 2010 we took this even further by setting new standards for easy deployment of security updates – creating Auto Update – following the pledge I made at RSA in 2009 to help users keep their systems up-to-date.

With all that has been learnt over the past year, the top priority for private and corporate users in 2011 should be to reduce the risks of vulnerabilities by applying unified patching, increasing awareness, and embracing the mantra of Vulnerability Management according to Aberdeen Group's Research Brief "Managing Vulnerabilities and Threats: No Anti-virus is Not Enough", December 2010: Assess, Prioritise, Remediate, and Repeat. It is our goal in 2011 to continue improving our solutions to help end-users and customers keep up-to-date and secure.

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

Patch & Stay Secure,

Niels Henrik Rasmussen
CEO

I. Secunia Vulnerability Intelligence

Overview

Vulnerabilities in software continue to be a major contributor to the risks people face when using the Internet. This report firstly provides an insight into the last five years of the security ecosystem with respect to vulnerabilities in software and then focuses on the year-on-year evolution of vulnerability data, comparing the data of 2009 with the data of 2010. Tracking vulnerabilities and the state of software security, the Secunia Vulnerability Intelligence database contains information about products from thousands of vendors; a formidable data-set to follow and assess the evolution of software security in an increasingly networked environment. Secunia validates, verifies, assesses, corrects, and tests the vulnerability information gathered with consistent and standard processes, which Secunia has constantly refined over the years. Besides the number of vulnerabilities in a specific group of programs, this report also investigates the evolution and the distribution of important vulnerability aspects; such as the criticality, the impact, the attack vector, the type of vulnerabilities, and the availability of patches.

Vulnerability statistics covering all products are a valuable benchmark for assessing the state and the evolution of software and the security ecosystem as a whole.

The security of information technology and computer networks is affected by a wide variety of factors and processes which together make up a complex and adaptive system. Whenever a new vulnerability is discovered, various parties with different and often conflicting motives and incentives become engaged in a complex way. In the last decade, the number of players and their roles and interactions within the security ecosystem has evolved considerably.
A variety of legislative and social issues directly influence the processes of vulnerability research, detection, publication, and response. Vendors, developers, customers, cybercriminals, and the security community have divergent perspectives on the impact of vulnerabilities. The processes and interactions between these factors are driven by the continuous discovery of new vulnerabilities and the subsequent constant need of the public (the software users) for vulnerability intelligence and patches.

An investigation into all vulnerabilities covering all products over a period of time reveals the evolution of the prevalence and interactions of some of these processes on a global scale.

For example:

- The total number of vulnerabilities affecting all products provides information on the on-going arms-race between vendors striving to produce secure software, and researchers' and cybercriminals' efforts (and successes) in finding new vulnerabilities in software
- The share of vulnerabilities with a patch available upon public disclosure indicates to what degree software vendors are able to coordinate and communicate with the security community
- The time from vulnerability disclosure to patch availability provides insights into the performance of vendors when acting upon new security issues and the risk exposure of software users
- The evolution of the type and impact of vulnerabilities indicates advances in the technology used to defend or attack software

Such information is valuable to assess and better understand the global state and evolution of software security. However, insights gained by examining all products are not necessarily applicable or particularly relevant to a specific group of software users. As organisations or individuals rarely deploy all software products available on the market, it is equally important and beneficial to focus the analysis on a specific and representative portfolio of products. In both business and private life, the largest group of Internet users are individuals working daily on their end-point PCs. To assess the exposure of this group, the analysis therefore focuses on the risks affecting the software portfolio found on a typical end-user machine in the second part of this report.

Secunia Advisories

Whenever a new vulnerability is reported a Secunia Advisory is released after verification of the information. A Secunia Advisory provides details, including description, risk rating, impact, attack vector, recommended mitigation, credits, references, and more for the vulnerability including additional details discovered during verification and testing, thus providing the information required to make appropriate decisions about how to protect systems. After the first publication the status of the vulnerability is tracked throughout its lifecycle and updates are made to the corresponding Secunia Advisory as new relevant information becomes available. For example, when the vendor releases a patch for the vulnerable product the status of the Security Advisory is changed to "patched". A Secunia Advisory is released or updated whenever new information becomes available, enabling the administrator of the vulnerable software to take appropriate action when needed. Several vulnerabilities released at the same time (if these vulnerabilities affect the same product and result in one administrative action) are reported in one Secunia Advisory. Likewise, several Secunia Advisories are released for a vulnerability affecting different products and requiring different administrative actions. Vulnerabilities are not reported in beta-versions of programs.

The number of Secunia Advisories published in a given period of time is a first order approximation of the number of security events in that period. Security events stand for the number of administrative actions required to keep the specific product secure throughout a given period of time.

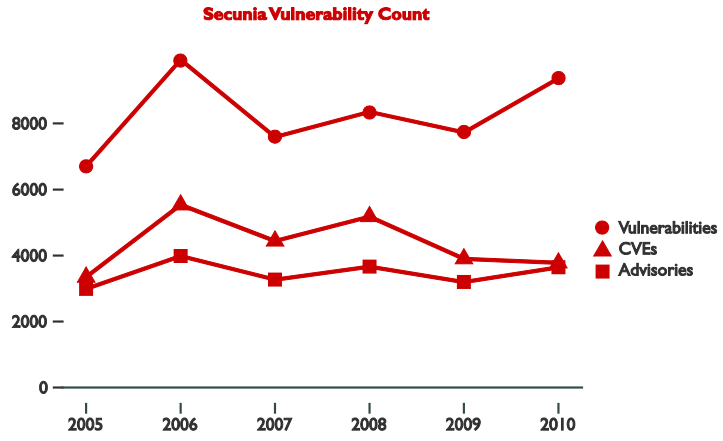


Figure 1 - Number of Vulnerabilities, CVEs, and Secunia Advisories per year since 2005.

Figure 1 shows the number of Secunia Advisories released in a given year since 2005 for all products in the Secunia Vulnerability Database. On average 3,460 Secunia Advisories were released per year from 2005 to 2010 with a standard deviation of 370 Secunia Advisories (11% of the average). A year-on-year analysis comparing the data from 2009 with the data of 2010 indicates an increase in the number of Secunia Advisories from 3,201 to 3,648 or 14%. This recent increase is slightly higher than the variance observed in the last five years. This analysis excluded "update for" Secunia Advisories for Linux distributions as these mostly are "duplicates" of already disclosed vulnerabilities for "upstream" products.

Vulnerability Counts and CVE

Common Vulnerabilities and Exposures (CVE)[1] is a de facto industry standard used to uniquely identify vulnerabilities which have achieved wide acceptance in the security industry. Using CVEs as vulnerability identifiers allows correlating information about vulnerabilities between different security products and services. CVE information is assigned in Secunia Advisories.

If CVE information becomes available after the release of a Secunia Advisory, it will be updated. Figure 1 shows the number of CVEs disclosed per year since 2005. On average 4,364 CVEs were reported per year in the Secunia Advisories from 2005 to 2010 with a standard deviation of 853 CVEs (20% of the average). More volatility was observed in the number of CVEs than in the number of Secunia Advisories per year. A year-on-year analysis comparing the data from 2009 with the data of 2010 indicates a slight decrease in the number of CVEs from 3,901 to 3,778 or 3%. This is 68% of the maximum number of CVEs observed in 2006.

> The Secunia Advisory count is a first order approximation of the number of Security Events, which is the number of administrative actions required to keep the specific product secure throughout a given period of time.
>
> CVE counts are a reasonable metric for the number of distinct vulnerabilities found in software.

When writing up a Secunia Advisory, a vulnerability count is added to each Secunia Advisory to indicate the number of vulnerabilities covered by the Secunia Advisory.

Using this count for statistical purposes is more accurate than, for example, counting CVE identifiers, which is often used as the best indicator available. The intention of CVE identifiers is, however, not to provide reliable vulnerability counts, but is instead a very useful, unique identifier for identifying one or more vulnerabilities and correlating them between different sources.

The problem in using CVE identifiers for counting vulnerabilities is that CVE abstraction rules (which has evolved over time to handle large variations in the amount of vulnerable details available) may merge vulnerabilities of the same type in the same product versions into a single CVE, resulting in one CVE sometimes covering multiple vulnerabilities. This may result in lower vulnerability counts than expected when basing statistics on the CVE identifiers.

Using vulnerability counts is, however, also not ideal as this is assigned per advisory. This means that one advisory may cover multiple products, but multiple advisories may also cover the same vulnerabilities in the same code-base shared across different programs and even different vendors.
Despite a vulnerability count being a technically more accurate metric, CVE identifiers have been used as a representation for the number of vulnerabilities in this report because these can be counted "uniquely" and CVE is the de facto industry standard for correlating different sources.

The graph in Figure 1 presents the correlation of Secunia Advisories, the vulnerability count, and CVE identifiers. It should also be noted that there were 1,600 Secunia Advisories issued in 2010 for which no CVE identifier is currently available. These will be updated as CVE identifiers become available. There were also around 900 CVE identifiers issued during 2010 which were not assigned to Secunia Advisories because these represented vulnerabilities in beta and development software, or are non-issues, e.g. fake and duplicate issues.

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

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

Vendors & Vulnerabilities

It is interesting to note that vulnerabilities are rather unevenly distributed among software vendors, as illustrated in Figure 2. Only a few software vendors account for the majority of the vulnerabilities. In the last two years, two vendors were responsible for 20% of the vulnerabilities, eight vendors for 40%, 46 vendors for 60%, and 465 vendors for 80% of all the vulnerabilities disclosed from 2009 to 2010. Thus, security investments by a few vendors can have a significant effect on the total number of vulnerabilities people are exposed to. Half of the vulnerabilities in the last two years were found in products by the following 14 vendors (in alphabetical order):

Adobe Systems, Apache Software Foundation, Apple, Cisco, Google, HP, IBM, Kernel.org, Microsoft, Mozilla Organization, Novell, Oracle[2], RealNetworks, and VMware

It is also noteworthy to mention that the products of these vendors are prevalent and in everyday use in businesses as well as on private computers.

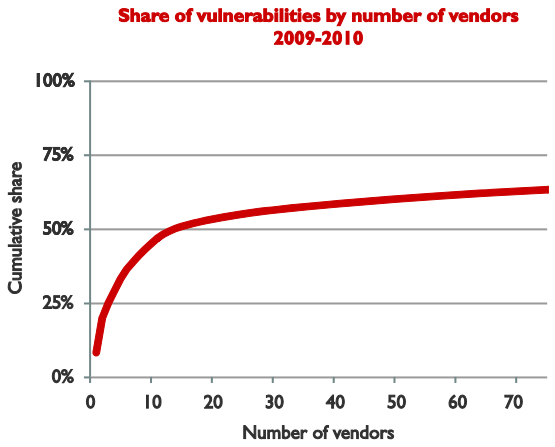


Figure 2 – Cumulative share of vulnerabilities from 2009-2010 by number of unique software vendors

In the last five years no significant upward or downward trend was observed, neither for the number of Secunia Advisories nor the number of CVEs disclosed. Thus, on a large scale, the security ecosystem appears to be in a state of equilibrium at the current rate of CVEs. Furthermore, this data shows that software vendors are still unable to release vulnerability free software at large – highlighting the continued need for effective vulnerability management for all types of software in use.

Year-on-Year Analysis – All Products

This section provides a year-on-year analysis of Secunia Advisories and vulnerabilities, comparing the evolution over the two recent 12 month periods; 2009 and 2010. This analysis further examines important vulnerability aspects such as the criticality, the impact, the attack vector, and the availability of patches in these periods.

[2] Oracle includes Sun Microsystem, BEA, and Peoplesoft as a result of recent acquisitions

Secunia Advisories and Vulnerability Count

Figure 3 and Figure 4 illustrate a year-on-year analysis of the cumulative number of Secunia Advisories and vulnerabilities (CVEs) respectively. The year-on-year analysis allows the tracking of short-term trends and identification of seasonal patterns in the timing of vulnerability disclosures. As can be seen in both Figure 3 and Figure 4 the data is evenly distributed in each 12 month period. When looking at all products from all vendors, no seasonal patterns are visible. This means that vulnerabilities are uniformly discovered and disclosed throughout the year. The increased trend in Secunia Advisories (+14% from 2009 to 2010) is also uniformly distributed between January and December and cannot be attributed to a single or a few distinct events.

As a specific "high season" for vulnerability disclosures cannot be identified, constant monitoring of the security environment throughout the year is a necessity in order to know the risks that software users are exposed to.

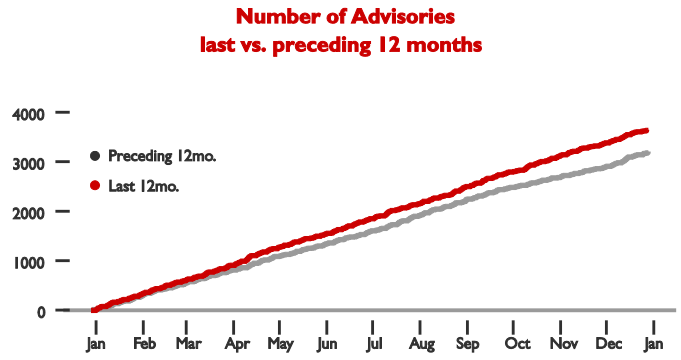


Figure 3 – Number of Secunia Advisories, last vs. preceding 12 months

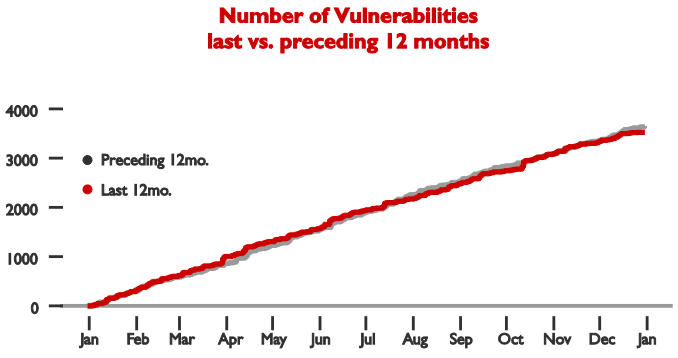


Figure 4 – Number of vulnerabilities (CVEs), last vs. preceding 12 months

Attack Vector

The attack vector describes the way an attacker can trigger or reach the vulnerability in a product. The attack vector is classified as "Local system", "Local network", or "From remote". The classification of attack vectors together with a description of how they are used in Secunia Advisories is listed in the Appendix of this report. Figure 5 plots a breakdown of the data by attack vector as a percentage of the total number of Secunia Advisories in the last and the preceding 12 months. It can be observed that "From remote" is consistently and by far the most prevalent attack vector in both 2009 and 2010 with at least a 84% share in each period, while "Local system" attributes to 8% and "Local network" to 8% in average over the last two years. Interestingly, the 14% increase in the number of Secunia Advisories from 2009 to 2010 can be almost uniquely attributed to the attack vector "From remote". Thus, the majority of the vulnerabilities expose the user of the software to remote attacks with an increased trend for this attack vector in 2010.

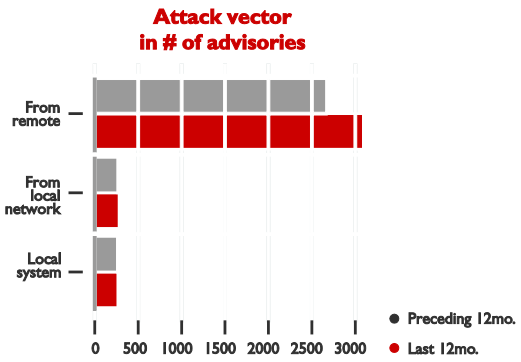


Figure 5 – Attack vector in number of Secunia Advisories, last vs. preceding 12 months

Criticality

The criticality of vulnerabilities is rated on a five-level criticality scale ranging from "Not critical" to "Extremely critical". The criticality of a vulnerability is based on the assessment of the vulnerability's potential impact on a system, the attack vector, mitigating factors, and if an exploit exists for the vulnerability and is being actively exploited prior to the release of a patch. The Appendix of this report lists the criticality classification together with a description of how they are used to rate the risk of a vulnerability.

Figure 6 shows that from 2009 to 2010 more than 58% of the advisories were rated "Highly" or "Moderately critical", while 37% were rated "Less critical", and only a very few were rated "Extremely critical" (5%). The distribution of the risk ratings has not changed substantially from 2009 to 2010. The 14% increase in the number of Secunia Advisories in 2010 is almost evenly distributed among the criticality classes "High", "Moderate", and "Less", while "Extreme" and "Not" remained almost the same.

The criticality of vulnerabilities depends considerably on the mix of products being examined. Figure 6 analyses 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.

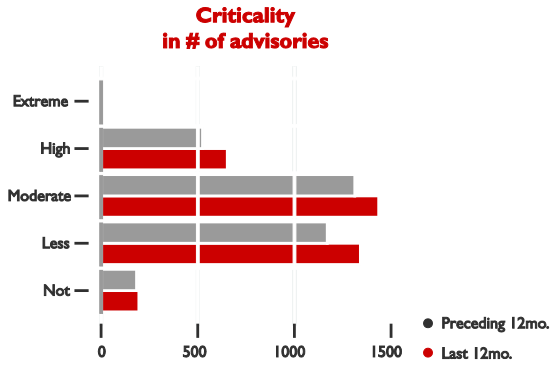


Figure 6 – Criticality in number of Secunia Advisories, last vs. preceding 12 months

Impact

This report 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 examined.

Figure 7 plots the distribution of the five most prevalent impact classes observed in 2010 and compares the numbers with the data from 2009. In the last two years the most prevalent impact class is "System access" with an average of 21% of the Secunia Advisories. System access allows an attacker to remotely execute arbitrary code or commands on the compromised system. Cross Site Scripting (XSS) is the second most prevalent impact class. Cross Site Scripting typically affects web applications and is rated as the number one vulnerability in the ranking of top web application vulnerabilities by the CWE top 25[3]. Denial of Service (DoS) is also ranked as one of the top impact classes in 2010 with 12%. This result demonstrates that many systems are vulnerable to attacks against the availability of the service or the process.

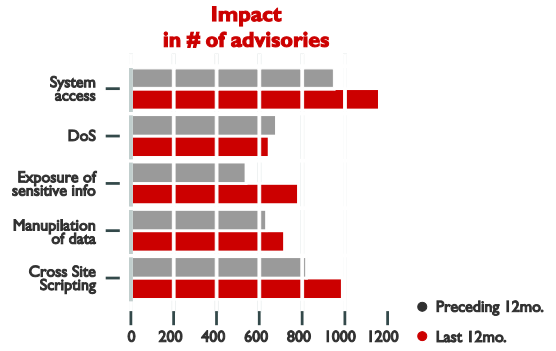


Figure 7 – Classification of the impact of successful exploitation of the affected system in number of Secunia Advisories, last vs. preceding 12 months

[3] CWE top 25 http://cwe.mitre.org/top25/

Solution Status & Patch Availability

This analysis tracks the remediation available for vulnerabilities through the solution status. If a patch from the vendor is available the solution status is marked "vendor patch". Otherwise the solution status is marked "unpatched" or "partial fix". A "partial fix" depicts a solution that is available but in one way or another is incomplete. It either covers only a subset of the vulnerabilities or it does not fix the vulnerability on all affected versions of the program. The "solution status" is updated as new information becomes available. For the two recent 12 months periods, Figure 8 reports the solution status at the disclosure date of the Secunia Advisory. As the solution status is reported on the day of disclosure, the number of advisories with status marked "vendor patch" indicates that the vendor had prior information about the vulnerability and was able to coordinate the release of the patch with the public disclosure of the vulnerability. This policy, called "coordinated disclosure", asks security researchers to submit their vulnerability discoveries directly to the affected vendor, and then hold off on disclosing details until a patch is available.

It can be observed that for roughly half of the advisories there is a patch available on the day of disclosure. This is an estimate for the prevalence of the "coordinated disclosure" process and the global data shows no change in prevalence from 2009 to 2010.

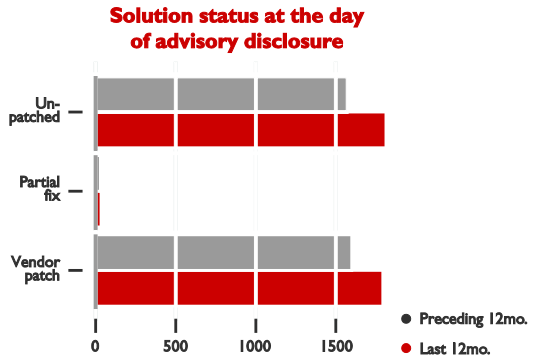


Figure 8 – Solution status on the day of advisory disclosure, last vs. preceding 12 months

Figure 9 further examines the delay from disclosure to patch release for all Secunia Advisories for which the vendor had no patch available on the day of disclosure. This analysis includes all patches released over the last 24 months. A patch was typically available within 30 days of disclosure for more than half of the remaining advisories. However, about a third of these Secunia Advisories were still unpatched after 60 days. The data of Figure 8 and Figure 9 for 2009 and 2010 is summarised in Table 1. Over a two year period, for 50% of the Secunia Advisories a patch was available at disclosure, for 22% a patch was made available later, and for 28% no patch was released at all. Note that a Secunia Advisory disclosed in December 2010 that gets patched in 2011 is counted as "unpatched" as only patches released before 2011 can be considered.

	Advisories	Share
Total Secunia Advisories 2009+2010	6,849	100%
Patch available at disclosure	3,401	50%
Patch available later	1,508	22%
No patch released in 2009+2010	1,931	28%

Table 1 – Summary of solution status and patch availability of Secunia Advisories 2009+2010

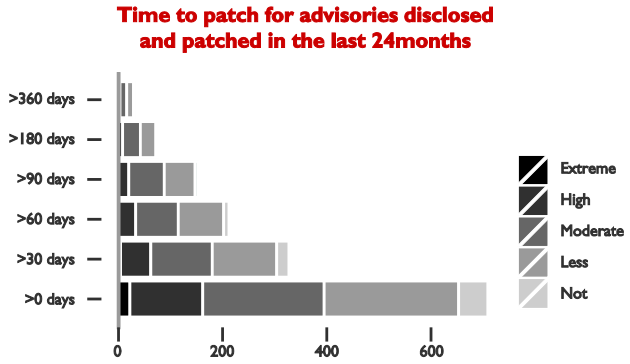


Figure 9 - Time to patch for advisories released and patched in the last 24 months

Advisories for products that are no longer supported by the vendor (end-of-life, EOL) at the reporting date are excluded from this analysis.

Conclusion

In summary, when looking at vulnerabilities covering all products, there were no major changes in the numbers and impact of vulnerabilities discovered over the last two years. The slight increase in the number of Secunia Advisories from 2009 to 2010 is within the variation observed over the last 5 years. The analysis of the attack vector, criticality, and the impact of vulnerabilities demonstrates that the majority of the vulnerabilities are relevant and pose a real risk to vulnerable systems. Furthermore, a patch is available on the day of disclosure for approximately half of the vulnerabilities, which means that the users of the software can remediate the vulnerability on the spot. For a large part of the remaining vulnerabilities a patch is released within 30 days of disclosure.

II. End-Point Host Security

The Top-50 Software Portfolio

The previous section of this report applied a bird's eye view perspective of all vulnerabilities. To obtain a better understanding of the risk and the security challenges most private or corporate Internet users face on a daily basis, this analysis now focuses on products typically found on end-point PCs and considers only those vulnerabilities. The variety and prevalence of programs found on typical end-point PCs, paired with the unpredictable usage patterns of users, make end-point PCs an attractive attack vector for cybercriminals. To assess these risks, a representative portfolio of software typically found on end-point PCs was built and its security tracked. Vulnerabilities on end-point PCs are commonly exploited when the user of the vulnerable computer visits a malicious website (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.

To obtain information about the software programs typically installed on end-points, anonymous scan results from the Secunia Personal Software Inspector (PSI)[4] are analysed. The Secunia PSI is a free program for identifying and reporting missing security patches and old program versions (end-of-life programs). Furthermore, the new release of the Secunia PSI 2.0 allows users to automatically and silently install patches for a growing number of popular programs. The Secunia PSI works by examining files on the user's PC (primarily .exe, .dll, and .ocx files). After examining all relevant files on the local hard drive(s), the collected data is matched against the file signatures engine to determine the exact version of the programs installed. The population of Secunia PSI users is constantly growing and reached over 3 Million installations in 2010. The following analysis is based on empirical data from users that frequently scanned their end-points with the Secunia PSI in 2010.

Results indicate that typically, 50% of the users have more than 66 programs from more than 22 different vendors installed[5]. Having software installed from 22 different vendors means that the user has to master approximately 22 different mechanisms to keep his/her end-point secure and patched. To assess the associated risk, a representative portfolio of the Top-50 most prevalent programs typically installed on end-point PCs was built.

This Top-50 group represents a typical user's software portfolio and contains programs from 14 different vendors, of which 26 programs are from Microsoft and 24 programs are from third-party (non-Microsoft) vendors. Each program in the Top-50 portfolio has at least a 24% prevalence. Eight programs from three vendors have more than a 80% user-share (e.g. Internet Explorer, .NET Framework, Sun/Oracle Java, Adobe Reader, and Adobe Flash). It is also worth noting that all the programs covered by the Secunia PSI span a massive 3,000 vendors.

[4] The Secunia Personal Software Inspector (PSI), http://secunia.com/psi
[5] Secunia Paper: "The Security Exposure of Software Portfolios", http://secunia.com/gfx/pdf/Secunia_RSA_Software_Portfolio_Security_Exposure.pdf

Operating System

Figure 10 examines the number of vulnerabilities in the Top-50 software portfolio together with the operating system Windows XP, Windows Vista, or Windows 7. This analysis reviews the same Top-50 portfolio of programs; however only combines it with different operating systems. The plot shows the data for the years 2009 and 2010 and the values are listed in Table 2. For Windows 7, released in October 2009, there is not enough data for the year 2009. There are two remarkable observations from Figure 10:

A) From 2009 to 2010 the number of vulnerabilities of the Top-50 portfolio including the operating system increased considerably, independent of the choice of operating system

B) The choice of the operating system has only a marginal effect on the total number of vulnerabilities affecting a typical end-point PC with the Top-50 Portfolio

The number of vulnerabilities in the portfolio in 2010 lies between a minimum of 709 with Windows 7 and a maximum of 729 with Windows XP. The choice of the operating system accounts for a difference of less than 3%. 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[6]. The number of Secunia Advisories is an estimated number of security events for the given portfolio. Table 2 reveals that the typical end-point was affected by between 148 to 163 security events due to vulnerabilities in the portfolio.

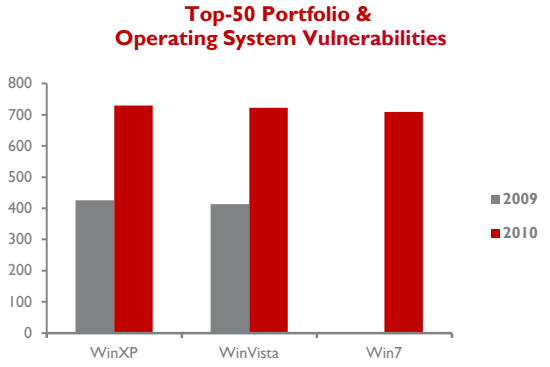


Figure 10 – Number of vulnerabilities of the Top-50 software portfolio including the operating System (Windows 7 was released in Oct 2009, no data for all 2009 available)

Secunia Advisories			
	2009	2010	Trend
Top-50 Portfolio + Windows XP	110	163	+48%
Top-50 Portfolio + Windows Vista	104	153	+47%
Top-50 Portfolio + Windows 7	N/A	148	N/A

Vulnerabilities			
	2009	2010	Trend
Top-50 Portfolio + Windows XP	426	729	+71%
Top-50 Portfolio + Windows Vista	413	722	+75%
Top-50 Portfolio + Windows 7	N/A	709	N/A

Table 2 – Number of Secunia Advisories and vulnerabilities of the Top-50 portfolio by operating system and year

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

Types of Vulnerabilities

This section of the report provides a detailed look into the types of vulnerabilities affecting the Top-50 portfolio with Windows XP. Windows XP was chosen as this is still the most prevalent end-point desktop operating system, and the difference between the operating systems is marginal. As in the first part of this report, this analysis focuses on the number of vulnerabilities, the attack vector, the criticality, the vulnerability impact, and the solution status of the vulnerabilities in the Top-50 portfolio with Windows XP.

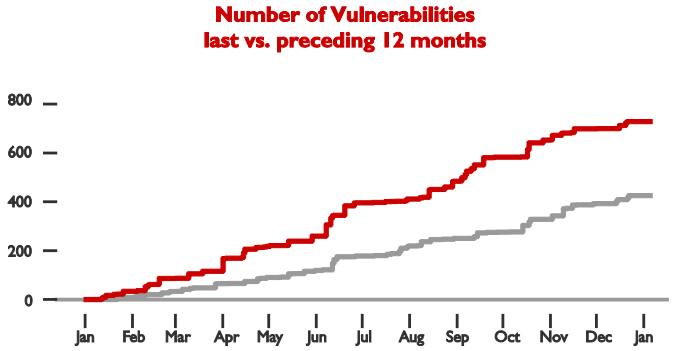


Figure 11 – Number of vulnerabilities of the Top-50 portfolio with Windows XP, last vs. preceding 12 months

Figure 11 shows the year-on-year analysis of the cumulative number of vulnerabilities for 2009 and 2010. A 71% increase in the number of vulnerabilities is clearly seen. There is an indication of seasonal patterns. In both years, early- to mid-June and October show an increased number of vulnerabilities. The increased activity in mid-June is followed by a four to six week period of almost no activity.

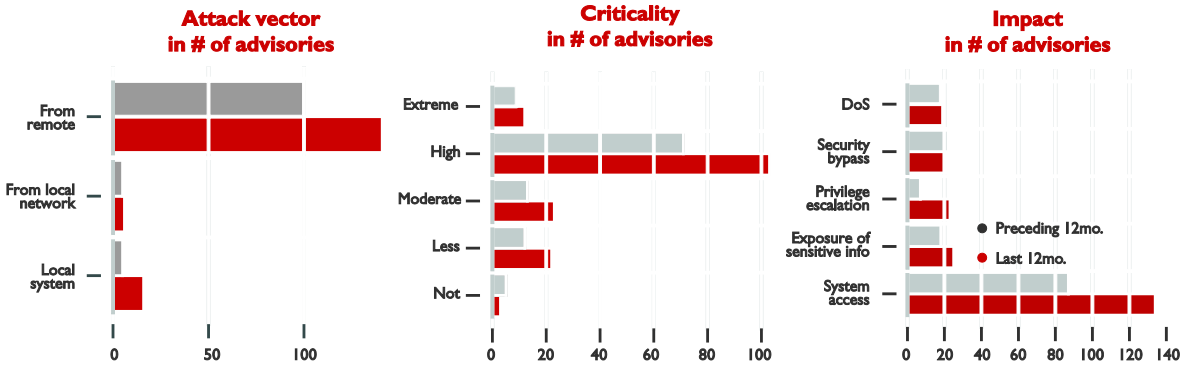


Figure 12 - Attack vector, criticality, and impact of the vulnerabilities of the Top-50 Portfolio with Windows XP, last vs. preceding 12 months

Figure 12 shows the attack vector, the criticality, and the impact of the vulnerabilities of the Top-50 portfolio with Windows XP. Similar to the results for all products, the majority (>95%) of the advisories are classified as "From remote". Furthermore, most of the increasing trends from 2009 to 2010 are also classified as "From remote". The criticality analysis shows that more than 70% of the advisories are classified as either "Highly critical" or "Extremely critical", whereas the classification "Highly critical" increased the most from 2009 to 2010. In addition, the impact classification reveals that more than 50% have "System access" as the impact.

These numbers clearly show that the vulnerabilities affecting a typical end-point are relevant and pose a real threat to the end-user's host.

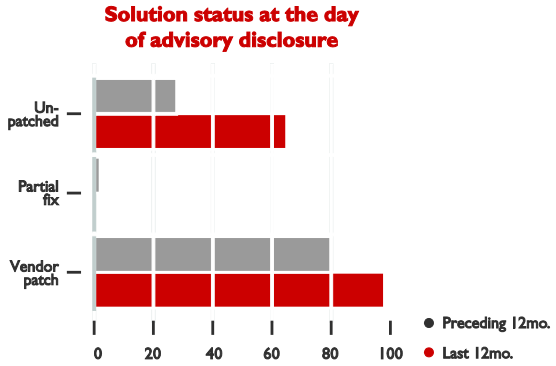


Figure 13 – Solution status of the advisories in the Top-50 portfolio and Windows XP on the day of disclosure. Last vs. preceding 12 months

Figure 13 shows the solution status of the Secunia Advisories of the Top-50 portfolio and Windows XP. It can be observed that more than half of the advisories had a patch available on the day of disclosure; namely 73% in 2009 and 60% in 2010. An analysis of the time from disclosure to patch availability, shown in Figure 14, reveals that for the majority of issues the vendors managed to release a patch within 30 days after disclosure.

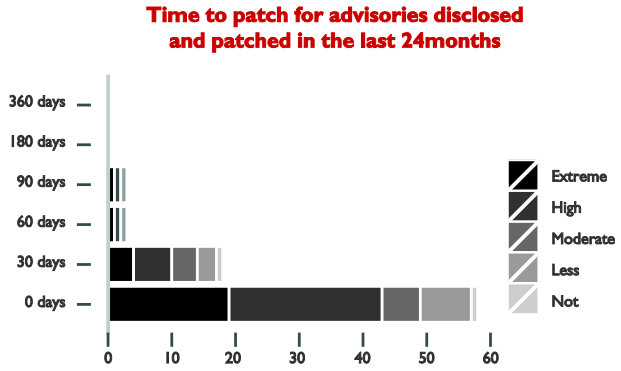


Figure 14 – Time to patch for advisories disclosed in the last 24 months Affecting the Top-50 Portfolio and Windows XP

In summary, the number and the severity of the vulnerabilities affecting a typical end-host increased from 2009 to 2010, and for about half of these vulnerabilities a patch was available on the day of disclosure.

Origin of Vulnerabilities

To understand the driver behind this increase in vulnerabilities affecting a typical end-point PC, the vulnerabilities are broken down according to their origin; that is by contributions from the Operating System (OS), from Microsoft programs (MS), and from Third-Party (TP) programs. The result is shown in Figure 15 for 2009 and 2010.

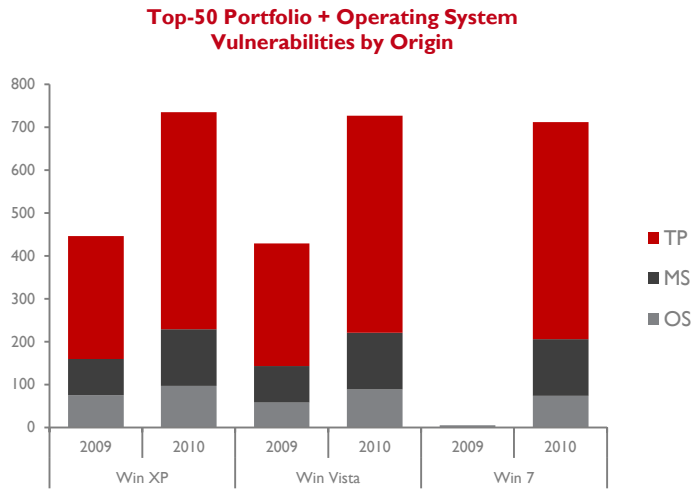


Figure 15 – Origin of vulnerabilities affecting a typical end-point PC in 2010, by Operating System (OS), Microsoft programs (MS), and Third-Party programs (TP)

Figure 15 shows that vulnerabilities in third-party programs by far outnumber vulnerabilities in the operating system or vulnerabilities in the Microsoft programs. This plot also reveals that the observed increase in vulnerabilities affecting a typical end-point PC is almost exclusively due to vulnerabilities by third-party products. In 2010 for example, an end-point PC with the Top-50 portfolio and Windows XP had:

- 3.83 times more vulnerabilities in the 24 third-party programs than in the 26 Microsoft programs
- 5.22 times more vulnerabilities in the 24 third-party programs than in the operating system

The numbers for the Top-50 portfolio and the operating systems are listed in Table 3.

Software Portfolio	TP/MS	TP/OS
Top-50 Portfolio + Windows XP	3.83	5.22
Top-50 Portfolio + Windows Vista	3.83	5.69
Top-50 Portfolio + Windows 7	3.83	6.84

Table 3 – Ratio between the numbers of vulnerabilities: Third-Party vs. Microsoft (TP/MS), Third-Party vs. Operating System (TP/OS)

Complexity of Patching the End-Point PC

The data for the Top-50 portfolio are remarkable as they provide an insight into the evolution of the risk exposure and the complexity of patching a typical end-point PC. Deployed software requires constant attention due to the continued discovery of new vulnerabilities and the release of patches. Upon the disclosure of a Secunia Advisory 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 required to keep specific products up-to-date, the number of Secunia Advisories are used as an approximation for the number of security events in a given period of time. Table 2 lists the numbers for 2009 and 2010, which highlight that a typical end-point PC is affected by approximately 150 security events per year.

The Top-50 portfolio contains 50 programs from 14 different vendors, namely 26 Microsoft programs and 24 third-party programs. The number of vendors also represents the number of different update mechanisms needed to keep this software portfolio up-to-date as vendors do not share update procedures and processes. Furthermore, many vendors still do not provide an easy to use and seamless mechanism to update their products. 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 the updating of programs on end-point PCs is largely neglected and left to the end-user.

In September 2010 and within the first 24 hours of the release of the Secunia PSI 2.0 beta, which includes the capability to automatically install patches for a growing number of programs; the Secunia PSI had installed approximately 10,000 security patches across 6,500 users or roughly 1.5 security patches per user on average. These initial results paint an interesting picture: At least six of the top ten programs patched by the Secunia PSI came with their own auto-update capability.

To highlight the complexity of patching, three examples of programs which usually prompt the user to accept the update (security related or not), were analysed:

Adobe Flash Player 10.x

Adobe Flash Player is used by 96% of all Secunia PSI users. During the beta phase, 35% of all beta testers had an Adobe Flash Player security patch automatically installed by the Secunia PSI Auto Update feature. Roughly 37% of the users with Adobe Flash Player installed, got their critical security patch from the Secunia PSI rather than from the vendor.

Sun Java JRE 1.6.x / 6.x

Sun Java is used by 79% of all Secunia PSI users. During the beta phase, 37% of all beta testers had a Sun Java security patch automatically installed by the Secunia PSI Auto Update feature. Roughly 47% of the users with Sun Java installed got their critical security patch from the Secunia PSI rather than from the vendor.

Adobe Reader 9.x

Adobe Reader is used by 63% of all Secunia PSI users. During the beta phase, 15% of all beta testers had an Adobe Reader security patch automatically installed by the Secunia PSI Auto Update feature. Roughly 24% of the users with Adobe Reader installed got their critical security patch from the Secunia PSI rather than from the vendor.

Thus, 37% of the users with Adobe Flash Player installed, 47% of the users with Sun Java installed, and 24% of the users with Adobe Reader installed got their critical security patch from the Secunia PSI rather than from the vendor. In other words, 37%, 47%, and 24% of these users would have been vulnerable for a substantial amount of time as the vendor failed to push the required security update to their end-users.

Furthermore, the end-user with the Top-50 software portfolio is required to master 14 different update mechanisms to patch a typical end-point with Windows XP:

- One update mechanism, namely Microsoft update, to patch the operating system and the 26 Microsoft programs. In 2010 this covered 31% of all vulnerabilities (down from 35% in 2009)
- Another 13 update mechanisms to patch the remaining 24 third-party programs from 13 different vendors. In 2010 these covered 69% of all vulnerabilities (up from 65% in 2009)

Typical users are either unaware, or simply overwhelmed by the complexity and frequency of the actions required to keep the dozens of third-party programs found on a typical end-point system secure.

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

- Users and businesses alike still perceive the operating system and Microsoft products to be the primary attack vector, largely ignoring third-party programs
- Many third-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

The difference in the level of Microsoft programs and third-party programs is real and measurable. Figure 16 measures the average share of insecure program installations found by the Secunia PSI in Q4 2010. The graph focuses on the group of the Top-10, 20, 30, 40, and 50 Microsoft programs and third-party programs. The results clearly show that Microsoft programs are more likely to be found patched on end-points than third party programs, which indicates that the complexity of patching has an impact on the patch level. Less than 2% of the Microsoft programs were found to be insecure while third-party programs ranked between 7% and 12%.

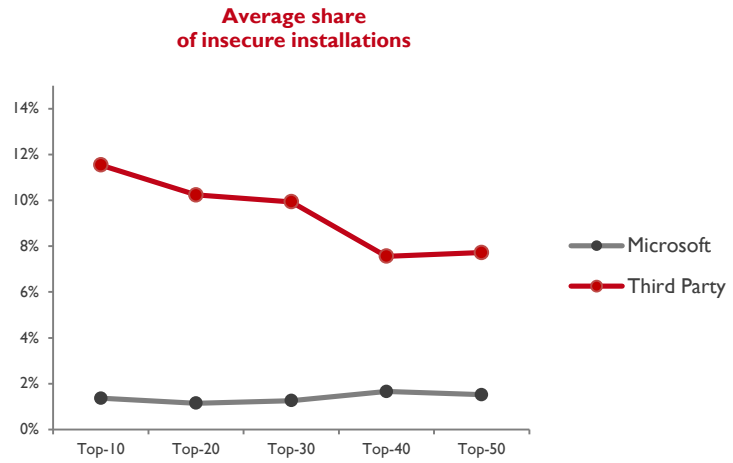


Figure 16 - Average share of insecure program versions installed in the Top-N Microsoft and Top-N Third-Party programs as seen by the Secunia PSI in Q4 2010

From an attacker's perspective, targeting third-party programs proves to be a rewarding path, and will probably remain so for an extended period of time. Only a few vendors such as Microsoft have the resources and expertise to consistently make the exploitation of their software harder, and to implement a formidable, "seamless", and easy to use auto-update mechanism to effectively relieve the users from the complexities of keeping their software up-to-date. Furthermore, as the number of security events and the complexity of the task increase, cybercriminals are handed a larger number of unpatched targets.

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 with ample time to exploit the vulnerabilities.[7] Therefore, focusing on third-party program exploitation will continue to provide attackers with a large pool of commonly used software that is easier to exploit[8], and much less likely to be found fully patched.

Today we are facing a challenging and complicated problem that is likely to take years to solve – the patching of third-party software.

[7] Paper: "Why Silent Updates Boost Security" http://www.techzoom.net/papers/browser_silent_updates_2009.pdf

[8] 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 risks that people are exposed to by using software and the Internet would certainly be by reducing the number of vulnerabilities and the window of opportunity to exploit vulnerabilities. By far the most effective way to reduce the risk of exposure is by reducing the complexity in patching the variety of programs typically found on end-point 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 third-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

In December 2010 Secunia released the Personal Software Inspector (PSI) 2.0 to help solve the problem of patching third-party software and significantly improve the security of home users' PCs. The Secunia PSI 2.0 features automatic updates that are truly automatic. Truly in the sense that, if the user prefers, the Secunia PSI 2.0 can install most security updates for a broad variety of programs without requiring the user to download, run, or otherwise perform manual actions to patch their PC.

It is important to note that a security patch provides better security than any number of anti-virus or other detection signatures as a patch eliminates the root cause. Anti-virus and perimeter protection are established and needed defence technologies which enjoy a high priority, whereas patching is typically seen as a secondary security measure. Effective patching should be prioritised according to the evolving threat landscape.

III. Quarterly Secunia Security Factsheets

Security vulnerabilities in software represent a particularly problematic risk to private and business users alike. However, the software industry still lacks coherent, standardised, and scheduled reporting of important security parameters for software products. In the finance industry, for example, key performance parameters are reported yearly or quarterly to consistently provide interested parties, and the public, with relevant information for decision-making and risk assessment.

Secunia has therefore created a new initiative to address the current lack of availability of relevant security information in a standardised and scheduled format: The Quarterly Secunia Security Factsheets.

Each Secunia Security Factsheet presents important security information of a given product in a concise and consistent format. The factsheets go well beyond simple vulnerability counts by analysing the type and number of vulnerabilities, paired with information about the software vendor's ability to roll out security patches. The information is based on Secunia's Vulnerability Intelligence database and analysis of its research.

The factsheets are released quarterly and provide the following key security parameters in a year-on-year (YoY) comparison:

- The number of advisories during the two recent 12 month periods (YoY)
- The number of vulnerabilities during the two recent 12 month periods (YoY)
- Breakdown by vulnerability attack vector in # of Secunia Advisories (YoY)
- Breakdown of vulnerability criticality in # of Secunia Advisories (YoY)
- Classification of the impact of successful exploitation on the affected system (YoY)
- Solution status (patched/unpatched) on the day of the Secunia Advisories disclosure (YoY)
- Information about the distribution of the time-to-patch, e.g. how many patches were released more than a given number of days after the disclosure of the vulnerability
- Historic evolution of Secunia Advisories and vulnerabilities for the last five years, including an extrapolation for the current year

Answering questions that would otherwise require extensive manual data mining is greatly facilitated by the new factsheets.

Secunia Security Factsheets cover more than a dozen major products and were first published in Q3 2010. Over time the number of products that the factsheets cover will continuously increase, based on customer and community feedback. The factsheets, including Q4 2010, are available at:

http://secunia.com/factsheets

The quarterly Secunia Security Factsheets will hopefully contribute to raising awareness on the evolution of threats, support customers in their work, and help spot new trends early.

IV. 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 exploits are in the wild. These vulnerabilities can exist in services like FTP, HTTP, and SMTP or in certain client systems like email programs or 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 known exploits available at the time of disclosure. Such vulnerabilities can exist in services like FTP, HTTP, and SMTP or in client systems like email programs or browsers.
Moderately Critical (3 of 5)	This rating is also used for vulnerabilities allowing system compromise on LANs in services like SMB, RPC, NFS, LPD and similar services that are not intended for use over the Internet. Typically used for remotely exploitable Denial of Service vulnerabilities against services like FTP, HTTP, and SMTP, and for vulnerabilities that allow system compromises but require user interaction.
Less Critical (2 of 5)	Typically used for cross-site scripting vulnerabilities and privilege escalation vulnerabilities. This rating is also used for vulnerabilities allowing the exposure of sensitive data to local users.
Not Critical (1 of 5)	Typically used for very limited privilege escalation vulnerabilities and locally exploitable Denial of Service vulnerabilities. This rating is also used for non-sensitive system information disclosure vulnerabilities (e.g. remote disclosure of installation path of applications).

Table 4: Vulnerability criticality rating as used in Secunia Advisories

Attack Vector Classification

Local System	Local System describes vulnerabilities where the attacker is required to be a local user on the system to trigger the vulnerability.
From Local Network	From Local Network describes vulnerabilities where the attacker is required to be situated on the same network as a vulnerable system (not necessarily a LAN). This category covers vulnerabilities in certain services (e.g. DHCP, RPC, administrative services) that should not be accessible from the Internet, but only from a local network or optionally from a restricted set of external systems.
From Remote	From Remote describes other vulnerabilities where the attacker is not required to have access to the system or a local network in order to exploit the vulnerability. This category covers services that are acceptable to be exposed and reachable to the Internet (e.g. HTTP, HTTPS, SMTP). It also covers client applications used on the Internet and certain vulnerabilities where it is reasonable to assume that a security conscious user can be tricked into performing certain actions.

Table 5: Vulnerability attack vector classification used by Secunia

Vulnerability Criticality 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 behaviour of a web application in a user's browser, 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 use a lot of memory) to crashing an application or an entire system.
Exposure of sensitive information	Vulnerabilities where 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 remotely 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 or administrative users. This typically includes cases where a local user on a client or server system can gain access to the administrator or root account, thus taking full control of the system.
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 are able to gain system access and execute arbitrary code with the privileges of a local user.
Unknown	Covers various weaknesses, security issues, and vulnerabilities not covered by the other impact types, or where the impact isn't known due to insufficient information from vendors and researchers.

Table 6: 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