ANALYST BRIEF – February 2013

VULNERABILITY THREAT TRENDS

A DECADE IN REVIEW, TRANSITION ON THE WAY

2013 – Stefan Frei, Ph.D.

Overview

After the close of 2012 NSS Labs performed a comprehensive analysis of vulnerability data to identify industry wide threats and trends covering the last 10 years. Despite massive security investments of the software industry, vulnerability disclosures have risen considerably in 2012. Several additional observations make the evolution of the year 2012 stand out significantly compared to the previous years since the peak in 2006. The parallel and massive drop of vulnerability disclosures by the two long established purchase programs iDefense VCP and TippingPoint ZDI indicate a transition in the way vulnerability and exploit information is handled in the industry.

Key Findings:

- The five year long trend in decreasing vulnerability disclosures ended abruptly in 2012 with a +12% increase
- More than 90 percent of the vulnerabilities disclosed are moderately or highly critical – and therefore relevant
- 9 percent of vulnerabilities disclosed in 2012 are extremely critical (with CVSS score>9.9) paired with low attack/exploitation complexity
- On average, around one percent of vendors account for 31 percent of the vulnerabilities disclosed per year
- Only one of the top 10 vendors managed to reduce vulnerability disclosures in 2012 compared to the average disclosures of the ten preceding years
- Microsoft and Apple operating system vulnerabilities decreased significantly from 2011 to 2012, by -56 per cent and -53 per cent respectively.
- Industry control systems (ICS/SCADA) saw more than six fold increase in vulnerabilities from 2010 to 2012

Recommendations:

- Identify, classify and prioritize mitigation of the most critical vulnerabilities as a security best practice.
- Identify and control access paths to ICS/SCADA systems. Prepare for attacks and related vulnerability disclosures
- Implement effective patch management programs wherever possible. Vulnerabilities in software will continue to be a major risk factor, increasing the importance of patch management in the critical path to security

This analyst brief was produced as part of NSS' independent testing information services. NSS received no vendor funding to produce this report.

Table of Contents

Table of Figures

Analysis

A vulnerability is a weakness in software that enables an attacker to compromise the integrity, availability, or confidentiality of the software or the data that it processes. The disclosure of the vulnerability is the admission of a software vulnerability to the public at large and does not refer to any type of private disclosure to a limited number of people or organizations. Typically disclosures can come from a variety of sources, such as the software vendor, security vendors, or independent researchers.

The data supporting this analysis is drawn heavily from NSS Labs' own research combined with the national vulnerability database (NVD)[1], an independent and publicly available repository of standards-based vulnerability management data operated by the U.S. government. The NVD represents all vulnerability disclosures that have a CVE (common vulnerabilities and exposures) identifier[2]. CVE is a de facto industry standard to uniquely identify and correlate vulnerabilities that has achieved wide acceptance in the security industry. Using CVE identifiers, the information about a vulnerability can be easily correlated to the respective security patches, exploit availability, or corresponding signatures in protection technologies such as intrusion prevention systems (IPS) or anti-virus engines.

Industry Wide Disclosures

This section of the report deals with the industry wide count of vulnerabilities covering all products, and their distribution among vendors and risk classes. As of January 2013 the NVD listed 53,489 vulnerabilities affecting 20,821 software products from 12,062 different software vendors. Figure 1 (top panel) illustrates the number of vulnerability disclosures across the software industry for each year since 2000, together with the number of software vendors and products affected by these vulnerabilities.

In the last ten years on average 4,660 vulnerabilities were disclosed per year, with an all-time high of 6,462 vulnerabilities counted in 2006 followed by a continued decrease for the next five years down to 4,139 (64% of the all-time high) in 2011.

However, in 2012 alone the number of vulnerabilities increased again to a considerable 5,225 (80% of the all-time high), which is 12% above the ten-year average. This is the largest increase observed in the past six years and ends the trend of moderate declines since 2006.

The yearly number of vendors and products affected by these vulnerabilities closely follows the shape of vulnerability disclosure numbers, as shown in Figure 1.

[1] NVD National Vulnerability Database - http://nvd.nist.gov

[2] CVE Common Vulnerabilities and Exposure - http://cve.mitre.org

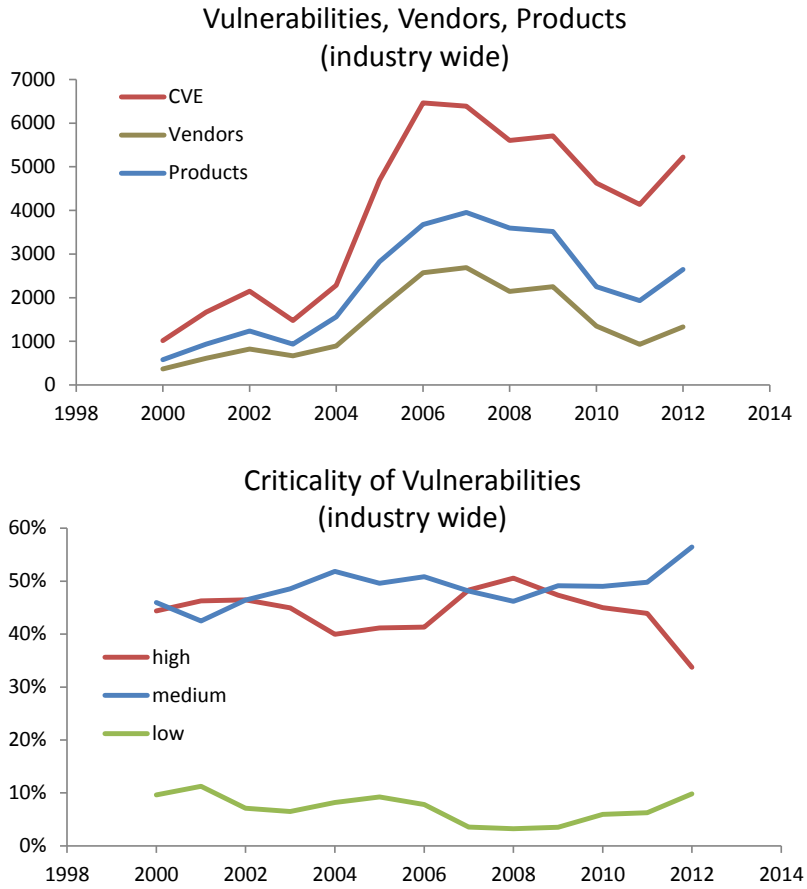

Figure 1 – Industry wide vulnerability disclosures and criticality distribution

Vulnerability Criticality

Figure 1 (bottom panel) also illustrates the distribution of the criticality of vulnerabilities disclosed since 2000. The criticality is rated as "high", "medium", or "low" based on the common vulnerability scoring system (CVSS)[3]. The CVSS base metric assigns a numeric value between 0 and 10 to vulnerabilities according to criticality, with higher scores indicating greater criticality:

- High criticality – vulnerability has a CVSS base score of 7.0 - 10.0
- Medium criticality – vulnerability has a CVSS base score of 4.0 - 6.9
- Low criticality – vulnerability has a CVSS base score of 0.0 - 3.9

The trend for highly critical vulnerabilities has been favorable since 2008 with a continued moderate decline from 51% in 2008 down to 34% in 2012, which is 10% below the ten-year average. This decline is offset by an increase of the shares of vulnerabilities with medium and low criticality to 50% and 6% in 2012 respectively. Vulnerabilities of

[3] CVSS Vulnerability scoring System - http://www.first.org/cvss

medium criticality again accounted for the largest number of disclosures at 2,949 in 2012. In the last decade on average 94% of the vulnerabilities were rated highly or moderately critical. Highly critical vulnerabilities with a CVSS base score of 9.9 or greater accounted for 9.3% of the vulnerabilities in 2012. Figure 1 covers more than a decade of security data and clearly illustrates that the majority of vulnerability disclosures are critical and therefore require immediate attention for business risk assessment; mitigating the most critical vulnerabilities first is a security best practice.

Attack Complexity

The complexity to execute a successful attack is an important factor to assess the risk of a vulnerability. A highly critical vulnerability that can only be exploited under very specific circumstances might require less immediate attention than a less critical vulnerability for which automated exploitation functionality is easily available in crimeware or penetration testing kits. The CVSS measures the complexity required to exploit the vulnerability once an attacker has gained access to the target system. The lower the required complexity, the higher the vulnerabilities' CVSS score.

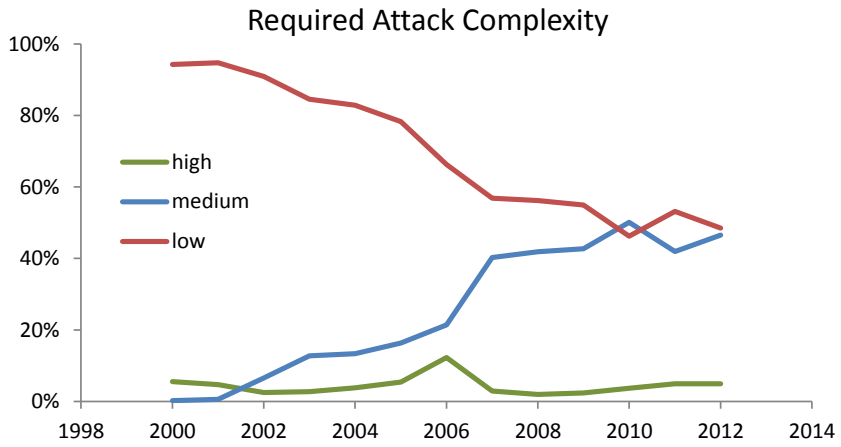

Figure 2 - Complexity required to successfully exploit a vulnerability. Low complexity indicates greater risk.

Figure 2 illustrates that the share of low complexity vulnerabilities – the easiest to exploit – repeatedly decreased from a high on over 90% early in the century to 48%,, or a total of 2,534 in 2012. In the same period medium-complexity vulnerabilities increased their share from below 5% to 47%, or 2,431, in 2012. Disclosures of high-complexity vulnerabilities have been mostly stable in the last decade at an average share of 4%. Figure 2 documents a clear (but slowing) trend towards an increase in attack complexity.

#	Vendor	CVEs	Share	Products
1	Adobe	112	23%	Flash-player, Adobe-AIR, Acrobat-Reader
2	Mozilla	64	13%	Firefox, Thunderbird
3	Oracle	47	10%	Java JRE, Fusion Middleware
4	Google	40	8%	Google Chrome
5	FFmpeg	28	6%	FFmpeg
6	HP	24	5%	Sitescope, Data-Protector-Express
7	Novell	9	2%	iPrint, Groupwise, File-Reporter
8	GoForAndroid	9	2%	Multiple Apps/Widgets
9	Advantech	8	2%	Web Access, Modbus-RTU-OPC-server
10	Microsoft	7	1%	Windows XP to 8, Internet Explorer

Table 1 – Top 10 vendors with highly critical, easy to exploit vulnerabilities with vendors' share of all such vulnerabilities disclosed in 2012.

Vulnerabilities with a high criticality paired with low attack complexity pose a clear and present threat to the user of the affected software. A considerable 484, or 9.2%, of the vulnerabilities disclosed in 2012 had a CVSS base score of 9.9 or more paired with a low attack complexity. For 2012, Table 1 lists the top 10 vendors and products affected by such vulnerabilities. The products affected by these vendors represent major types software in everyday private and business use, such as popular web browsers, plugins and media players, or operating systems. One notable exception is Advantech, a producer of industry control/SCADA systems.

Distribution of Vendors and Vulnerabilities

Categorizing and examining the distribution of the vendors affected by vulnerability disclosures provides deeper insight into the threats and trends.

The distribution of vulnerabilities among vendors is skewed, with only a few vendors accounting for the majority of vulnerability disclosures every year. Figure 3 illustrates the share of the top 1, top 10, top 100, and top 500 vendors with most vulnerabilities disclosed per year. Over the last decade, the top 10 vendors accounted on average for 31% of all disclosures in a given year; the top single vendor accounts on average for 7% of the disclosures per year. Up to 2006, the share of the top vendors declines, and rises again thereafter to peak in 2011. This matches the observation in Figure 1, which shows an increase of the number of vendors up to 2006 followed by a decline. With only a few vendors accounting for the majority of vulnerabilities, the security investment by a few vendors can have a significant effect on the industry and the number of users affected by vulnerabilities.

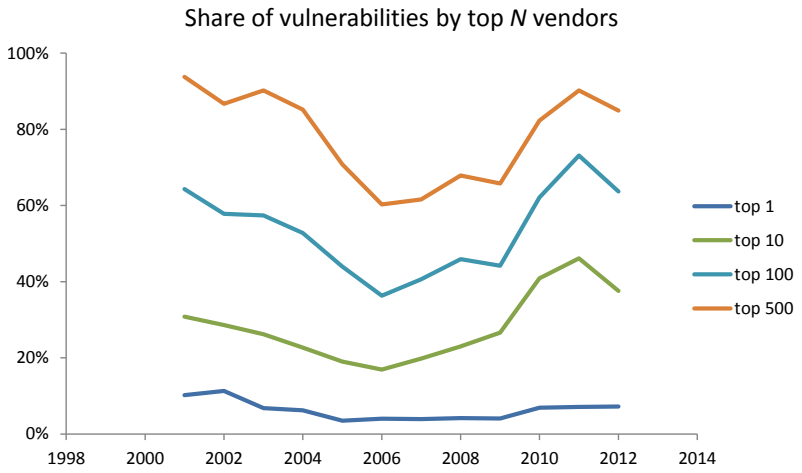

Figure 3 – Share of vulnerabilities of the top N vendors with the most vulnerabilities per year

Differentiating *new* vs. *recurring* vendors reveals another trend. A vendor that was seen to be vulnerable in year (Y) but not in any of the previous two years (Y-2, Y-1) is considered as a new vendor. New vendors either just entered the software market or their products are only occasionally affected by vulnerabilities. Recurring vendors, on the other hand, are vendors that were found vulnerable in year (Y) and either of the two preceding years (Y-2, Y-1).

The vulnerabilities disclosed in 2012 affected 2,646 products from 1,330 different vendors. A considerable 976 or 73% of these vendors were new in 2012. These new vendors accounted for 30% of the vulnerabilities disclosed in 2012.

Over the last ten years NSS noted an average of 69% new vendors and 31% recurring vendors per year. This entry/exit dynamic is illustrated in Figure 4. The left panel documents the yearly share of new and recurring vendors. From 2005 to 2011 the share of new vendors declines moderately from 76% to 59%, only to rise abruptly in 2012 to 73%. For new vendors there is, on average, a stable ratio of 1.5 vulnerabilities per vendor. For recurring vendors, however, the ratio of vulnerabilities per vendor is considerably higher. In a first phase from 2004 to 2009 this ratio is stable at 5.2 vulnerabilities per vendor. Thereafter, as documented in the right panel in Figure 4, the ratio rises consistently and considerably to 10.6 in 2012, more than double the value in the first phase.

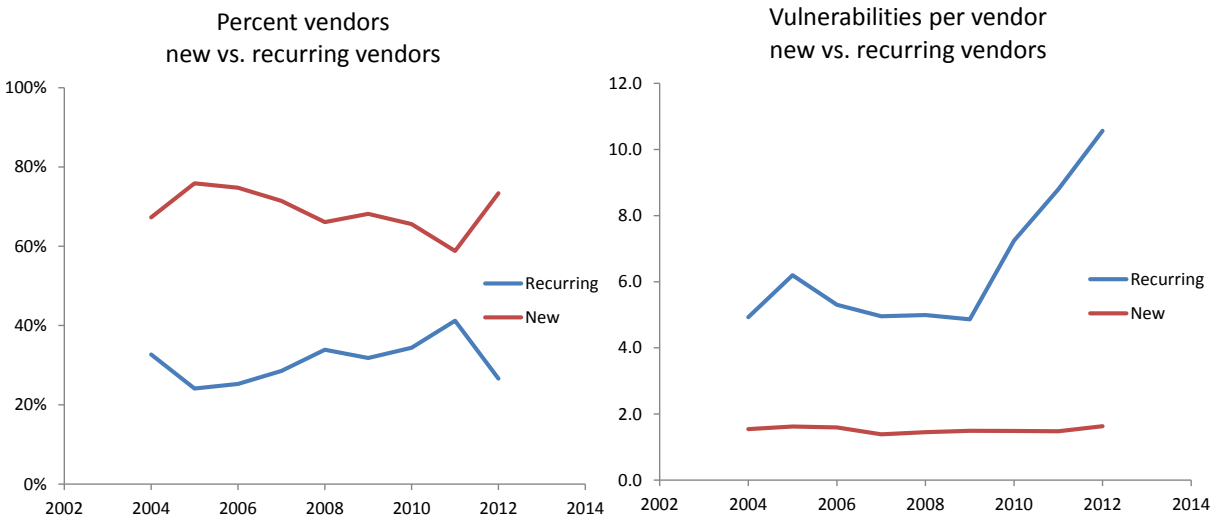

Figure 4 - Percent new and existing vendors found vulnerable in a given year.

Thus, the number of vulnerabilities per recurring vender has been on the rise since 2009. This can also be seen in Table 2, which lists the top 10 vendors by vulnerability disclosures in 2012 together with their history and 10-year/1-year trend. The year with the highest vulnerability count is marked in each vendors plot.

Compared to the average numbers of the preceding 10 years, only one of these 10 vendors managed to decrease the number vulnerability disclosures in its products in 2012. All other vendors increased their vulnerability numbers in 2012, thereby also increasing the vulnerabilities/vendor ratio.

#	Vendor Name	History 2002-2012	Average 2002-2011	Vulnerabilities 2011	Vulnerabilities 2012	Trend 10 year	Trend 1 year
1	Oracle		240	342	429		
2	Apple		160	253	297		
3	Google		52	294	279		
4	Mozilla		87	116	202		
5	IBM		113	168	175		
6	Microsoft		221	254	172		
16	Readhat		112	128	162		
7	Cisco		93	167	160		
8	Adobe		72	200	146		
23	Novell		113	177	145		
9	Linux		76	86	115		
10	Moodle		7	2	94		

Table 2 – Top 10 vendors by vulnerability disclosures in 2012[4]

[4] Oracle contains Sun and BEA since the mergers, linux based operating systems contain linux and linux kernel vulnerabilities.

Selected Software Portfolios

Analyzing industry wide vulnerability disclosures covering all products from all vendors includes a large number of rare products and web applications that are not in typical everyday business or private use. In this section we therefore analyse different software portfolios to highlight specific areas of interest.

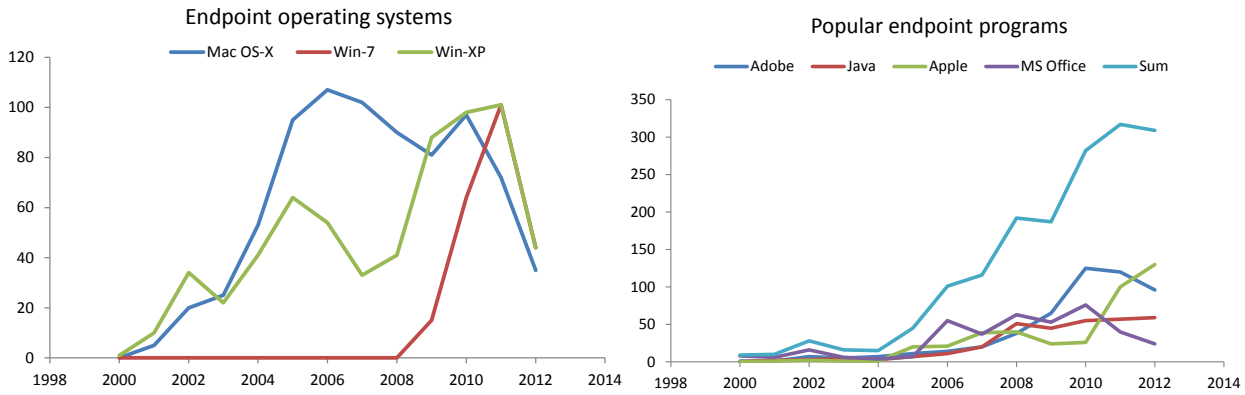

Figure 5 – Endpoint operating systems (left) – endpoint popular programs (right)

Endpoints

Windows operating systems still dominate the industry with an estimated market share of around 90%, followed by Apple's Mac OS X operating system estimated at around 7% market share at the end of 2012. The left panel in Figure 5 illustrates that 2012 marked the year of the largest decrease in vulnerability counts for these operating systems. Vulnerability numbers dropped from their all time high of 101 in 2011 down to 44 in 2012 for both Windows 7 (released in 2009) and the older Windows XP (released in 2001.) A similar trend is observed for the Apple operating system. A significant downward trend started in 2010 at 97 vulnerability disclosures (the all time high was at 107 in 2006) down to 35 in 2012.

Typical applications found on the majority of endpoint systems are web browsers and:

- From Adobe: Flash Player, Acrobat Reader
- From Oracle/Sun: Java
- From Apple: iTunes, Quicklime Player
- From Microsoft: MS-Office, Word, Excel, PowerPoint

The right panel in Figure 5 tracks vulnerability disclosures of the above popular programs, and their sum. Vulnerabilities in Microsoft Office and the Adobe programs started to decline since 2010, while Java increased slightly. The Apple applications, however, suffered a major increase since 2010. Comparing 2011 with 2012:

- Adobe programs reduced vulnerabilities by -20% (from 120 to 96)
- MS-Office programs reduced vulnerabilities by -40% (from 40 to 24)
- Oracle/Sun Java increased vulnerabilities by +4% (from 57 to 59)
- Apple programs increased vulnerabilities by +30% (from 100 to 130)

In total, the combined vulnerability numbers of these components decreased slightly by -3% (from 317 to 309) from 2011 to 2012. Thus, the vulnerabilities in the operating system only represent a fraction of the total vulnerabilities of a typical endpoint. Patching the operating system alone is not enough.

Web browser

Web browsers are the most used and most prevalent programs to access the Internet. The left pane in Figure 6 illustrates the vulnerability disclosures of the four most prevalent web browsers: Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari. In the years since the release of Google Chrome in 2008, all but Internet Explorer increased the number of vulnerability disclosures. For the first time since its launch in 2008, Google Chrome saw a decrease in vulnerability disclosures from 2011 to 2012. There is a considerable difference in the number of vulnerability disclosures amongst the browsers of over 200 vulnerabilities in 2012.

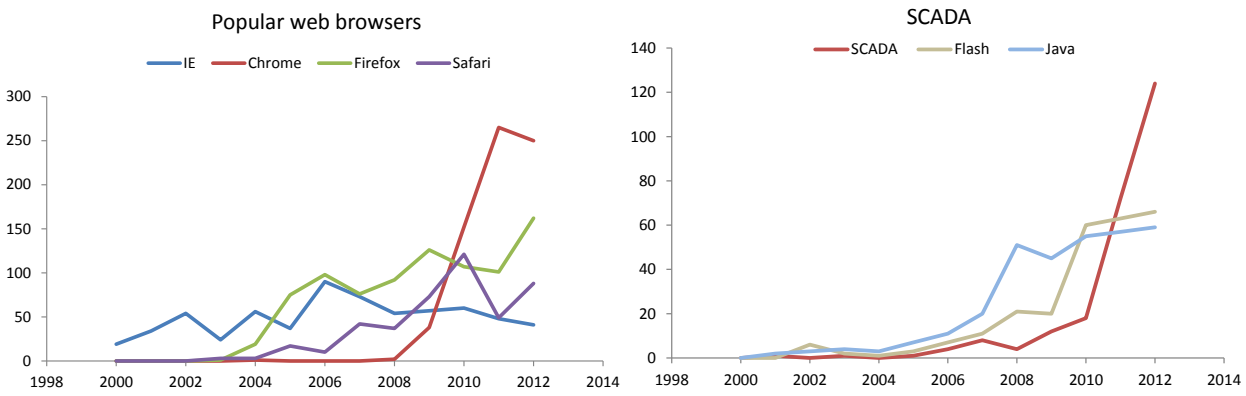

Figure 6 – Web browsers (left) – control systems/SCADA (right)

Industrial Control Systems/SCADA

SCADA (supervisory control and data acquisition) is a type of industrial control system (ICS). Industrial control systems are computer-controlled systems that monitor and control industrial processes in the physical world. SCADA systems are significantly important systems used in national infrastructures. These systems control industrial, infrastructure, and facility-based processes such as electric grids, water supplies, power plants, pipelines, etc.

The security of SCADA systems has been under intense scrutiny since 2010 following the discovery of the computer viruses Stuxnet and Flame. This increased interest in ICS product security has also resulted in a significant increase in product vulnerability reports. The right pane in Figure 6 documents the explosion of vulnerability reports affecting ICS/CADA systems since 2010. For comparison, the sudden rise of Java and Adobe Flash vulnerabilities starting around 2006 is plotted in the same chart. This clearly demonstrates the scale of this trend.

ICS/SCADA vulnerability disclosures increased more than 600% since 2010 and almost doubled from 72 in 2011 to 124 in 2012. These 124 vulnerabilities affect the products of 49 vendors; the top 20 are listed in Table 3.

#	Vendor	CVEs	#	Vendor	CVEs
1	Siemens	31	11	Cogentdatahub	6
2	Advantech	24	12	Cisco	6
3	Invensys	16	13	Ecava	6
4	GE	12	14	Indusoft	6
5	Rockwell Automation	11	15	Intellicom	6
6	Wellintech	11	16	Koyo	5
7	Sielcosistemi	10	17	Iconics	5
8	7t	10	18	Progea	5
9	Windriver	7	19	Measuresoft	5
10	Schneider-Electric	6	20	Areva	5

Table 3 – Top 20 vendors of industry control systems (ICS) by vulnerability disclosures

In 2012 security researchers and others have released tools to facilitate the identification of Internet facing ICS and the exploitation of vulnerabilities identified in these systems. The security arms race has just started and we expect vulnerabilities and security issues in ICS/SCADA systems to increase and continue to trouble the industry in the years to come.

Vulnerability Markets

Information about security vulnerabilities can be a valuable asset. Vulnerability information is traded via the underground “black market" and commercial services. Vulnerability commercialization remains a hotly debated topic tied to the concept of vulnerability disclosure. Coordinated (or responsible) disclosure fails to satisfy security researchers who expect to be financially compensated, even though reporting vulnerabilities to the vendor with the expectation of compensation might be viewed as extortion. On the other hand, cybercriminals not bound by legal or ethical considerations are willing to invest considerable amounts in suitable vulnerability information.

The year 2012 saw many reports regarding a change and expansion of vulnerability and exploit markets. More software vendors started to offer (or increased) rewards to researchers submitting their findings. At the same time, new and existing companies engaged in vulnerability or exploit markets received significant press attention, either because of their findings or by winning hacking contests. The way vulnerability information is handled has undergone a transition, and vulnerability markets are rapidly expanding in 2012[5].

Traditionally the two primary players in the commercial vulnerability market are iDefense, which started its vulnerability contributor program (VCP) in 2003, and TippingPoint, with its zero-day initiative (ZDI) started in 2005. These services openly advertise their vulnerability handling policies. Demonstrating and ensuring that buyers and sellers don't have malicious intent is a major challenge for them.

These buyers typically purchase vulnerability information to protect their customers before the vulnerability becomes public knowledge, and then inform the vendor of the affected software. VCP and ZDI advertise their ethics and ask security researchers to accept lower compensation with the promise that the information will be used for benevolent purposes.

[5] Forbes Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits - http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

Vulnerability prices are not disclosed but ZDI runs a "frequent-flyer" style program that can pay out bonuses as high as $20k to top researchers. Following their inception and up to 2012, VCP and ZDI published 1,604 vulnerabilities (99% of which are rated as highly critical) affecting 211 different vendors.

Figure 7 illustrates the combined share of ZDI and VCP purchases on the total vulnerability disclosures per year for highly critical vulnerabilities. The average since 2005 (inception of ZDI) is 7.0% of all highly critical vulnerabilities. There is a remarkable all time high in 2011 at 18%, followed by a fall to 6.3% in 2012. Figure 7 illustrates a steady rise of share in the years 2006 to 2011, followed by a sharp fall in 2012.

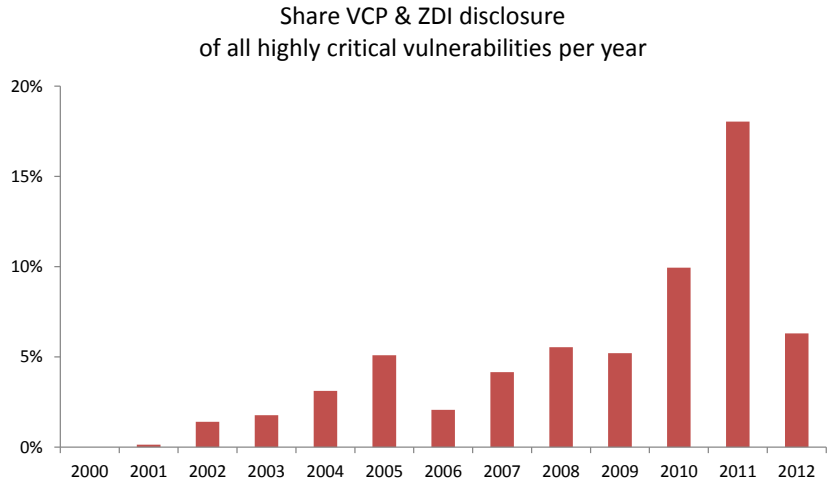

Figure 7 – Combined share of commercial vulnerability purchase programs ZDI & VCP

Figure 8 lists the top 10 vendors for which VCP and ZDI respectively bought vulnerabilities. These two lists have eight vendors in common. For both programs, 18% of their purchases were for vulnerabilities in Microsoft applications.

ZDI - Top 10 Vendors

#	Vendor	CVEs	Share
1	Microsoft	162	18%
2	Apple	145	16%
3	HP	89	10%
4	Adobe	75	8%
5	RealNetworks	67	8%
6	Novell	57	6%
7	Sun	46	5%
8	Mozilla	45	5%
9	IBM	34	4%
10	Oracle	27	3%

VCP- Top 10 Vendors

#	Vendor	CVEs	Share
1	Microsoft	131	18%
2	Adobe	49	7%
3	Apple	47	6%
4	IBM	38	5%
5	Sun	29	4%
6	symantec	24	3%
7	CA	22	3%
8	Novell	21	3%
9	RealNetworks	21	3%
10	Oracle	18	3%

Figure 8 – Top 10 vendors for which ZDI & VCP purchased vulnerabilities since 2001

The sharp fall of the combined share of the long established programs VCP and ZDI observed in 2012 correlates with reports of the vulnerability and exploit market rapidly expanding in 2012. These changes in the security industry likely affect the share of established programs, and could change the dynamics of the vulnerability handling processes in the future.

Conclusion

Based on the analysis of vulnerability disclosure data since 2002 we find that the year 2012 stands out significantly compared to the evolution of the previous years following 2006. The following observations regarding the year 2012 are particularly noteworthy:

a) The five year long trend in decreasing vulnerability disclosures ended abruptly in 2012 with a trend reversal initiated by a sudden +12% rise
b) Both Microsoft and Apple operating systems saw their largest fall in vulnerability disclosures of the last 10 years
c) Both vulnerability purchase programs VCP and ZDI reversed their five year long rise with a reduction of more than 50% of vulnerability disclosures in 2012
d) A significant increase in new vendors found vulnerable in 2012

These observations paired with the changing way and increasing options of how vulnerability or exploit information is handled support the notion that the security industry currently undergoes transition.

Contact Information

NSS, Inc.
6207 Bee Caves Road, Suite 350
Austin, TX 78746 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com