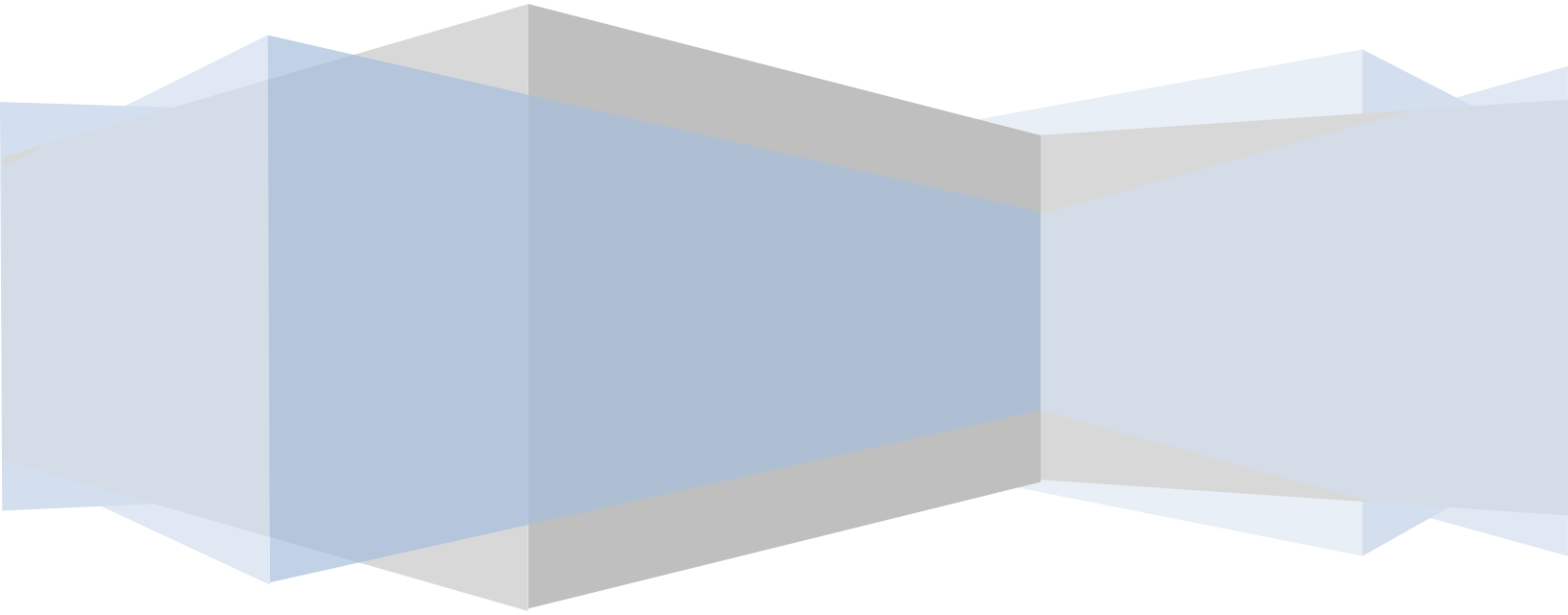
iViZ Security Inc

(In) Security in Security Products 2013



©iViZ Security Inc 2013

Introduction

We use security products to secure our systems and our businesses. However, the very security products we use, can themselves have vulnerabilities which can leave us susceptible to attacks. In this annual report iViZ studies the vulnerability trends in security products.

In our last year's report, we published trends in major security products and security vendors. We concluded with the fact that security products and vendors are as vulnerable and insecure as are any other products and vendors respectively. We took some time to find out what were the major security breaches over the last couple of years and the results are quite interesting. In 2012 alone, some major security vendors like Symantec Corporation, GlobalCerts and Panda Security among others got targeted and breached by attackers.

Here is a summary of some recent major events of Security companies that got hacked.

Symantec Corporation -Security software giant attacked by anonymous hacker in Jan 2012

- The company had source code stolenfor software titles like Norton Antivirus corporate edition, Norton Internet security, Norton Utilities, Norton GoBack and pcAnywhere.
- They were hacked again in November with the complete database from the Symantec online portal leaked.
- Their employee's database containing email addresses and passwords was breachedwith the loss of around 3,195 records.

Panda Security, a cloud security company was hacked by LulzSec and the hacking group Anonymous in Mar 2012

- Multiple usernames and passwords of employees were breached.
- Atleast 35 of their public facing websites hacked.

GlobalCerts, a firm which provides Email Security Solutions hacked by an anonymous hacker in Aug 2012

- Database hacked with over 1000 client details leaked.
- Critical information like Usernames, emails, passwords, company and personal information compromised.

Barracuda Networks-embarrassed by hacker database break-in.

- Barracuda took down their firewall for maintenance for no more than a few hours during which time an attacker was able to infiltrate their systems.
- The attacker discovered an SQL injection flaw in a PHP script used to display customer case studies.
- The attacker was able to get employee passwords that were encrypted using a MD5 hashing algorithm, which is considered, outdated by today's standards.

It is evident that compromising a security company may lead to some kind of chain of security breaches all around the world. There are also various examples of critical vulnerabilities discovered in security products including anti-virus, firewalls and backup software, as shown below:

AntiVirus

- The decomposer engine in Symantec Endpoint Protection (SEP) 11.0, Symantec Endpoint Protection Small Business Edition 12.0, Symantec AntiVirus Corporate Edition (SAVCE) 10.x, and Symantec Scan Engine (SSE) before 5.2.8 does not properly perform bounds checks of the contents of CAB archives, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted file.

- The Antivirus component in Comodo Internet Security before 5.3.175888.1227 does not properly check whether unspecified X.509 certificates are revoked, which has unknown impact and remote attack vectors.

- **iViZ Security** has discovered **remote code execution vulnerabilities** in various anti-virus products including AVG, F-Secure, Sophos and ClaimAV etc. See here for more details.

- **iViZ Security** has discovered **data stealing vulnerabilities** in the major disk encryption applications including **Microsoft Bitlocker, TrueCrypt and Mcafee Safe Boot Device**. See here for more details.

Firewall

- The auth-proxy functionality in Cisco Firewall Services Module (FWSM) software 3.1 and 3.2 before 3.2(20.1), 4.0 before 4.0(15.2), and 4.1 before 4.1(5.1) allows remote attackers to cause a denial of service (device reload) via a crafted URL, aka Bug ID CSCtg02624.

- Memory leak in Cisco IOS 12.2, 12.4, 15.0, and 15.1, when Zone-Based Policy Firewall SIP application layer gateway inspection is enabled, allows remote attackers to cause a denial of service (memory consumption or device reload) via malformed SIP messages, aka Bug ID CSCtl99174.

- The web interface in McAfee Firewall Reporter before 5.1.0.13 does not properly implement cookie authentication, which allows remote attackers to obtain access, and disable anti-virus functionality, via an HTTP request.

- A race condition in the Zone-Based Firewall in Cisco IOS 15.1 and 15.2, when IPS policies are configured, allows remote attackers to cause a denial of service (device crash) by sending IPv6 packets, aka Bug ID CSCtk53534.

- The default configuration of the NETGEAR ProSafe FVS318N firewall enables web-based administration on the WAN interface, which allows remote attackers to establish an HTTP connection and possibly have unspecified other impact via unknown vectors.

- The web server on the Siemens Scalance S Security Module firewall S602 V2, S612 V2, and S613 V2 with firmware before 2.3.0.3 does not limit the rate of authentication attempts, which makes it easier for remote attackers to obtain access via a brute-force attack on the administrative password.

Backup Software

- **Man in the Middle (MITM**) vulnerability in **Symantec BackupExec** 12.1 and other versions. The vulnerability allows stealing confidential data from the Symantec Backup software.

- Directory traversal vulnerability in the Management Console on the Symantec NetBackup (NBU) appliance 2.0.x allows remote attackers to read arbitrary files via unspecified vectors.

It is also quite evident that security products are vulnerable to same type of vulnerabilities such as Buffer Overflow, MITM, Information leakage etc. as any other products used in the organizations. In the next few sections, we will explore vulnerability trends in various security products in more details.

It is also worth noting some of the assumptions we took to compile the result. In our research, we have referred to well-known vulnerability standards and databases like Common Vulnerability Enumeration (CVE), Common Product Enumeration (CPE) and Nation Vulnerability Database (NVD). One of the major challenges we faced is in classifying the products into security and non-security products, as the current product standard (CPE) does not support it. We solved this challenge by using keyword based learning algorithm based upon the fact that security products have certain keywords like ‘virus’, ‘firewall’, ‘ IDS ‘, ‘ IPS ‘, ‘scan’ etc. Our statistics are also based upon the latest vulnerability data; NVD updates its vulnerability database almost daily.

Vulnerability Trend in All Products

Figure **1** Shows the trend of publicly disclosed vulnerabilities across all software products for the past 15 years. As shown in the graph, in 2012 there was a sharp increase in the number of vulnerabilities.

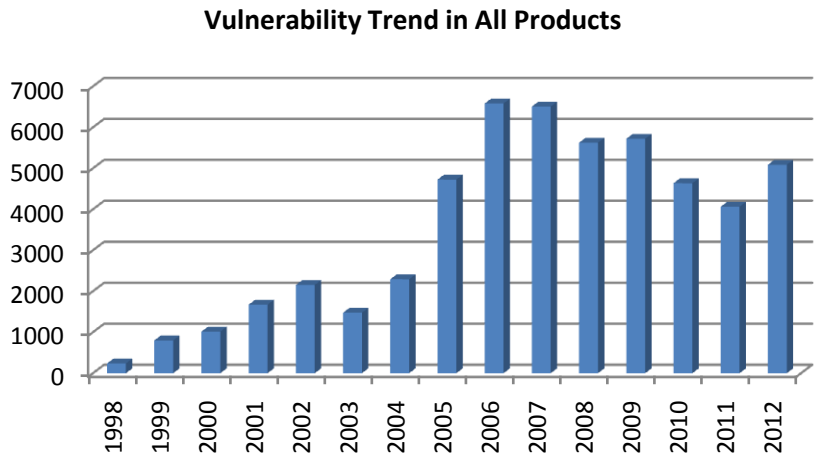


Figure 1: Shows vulnerability findings in all the known and documented products. Y axis shows number of vulnerabilities discovered. X axis shows respective consecutive years.

Vulnerability Trend in Security Products

Figure 2 Shows trend of publicly disclosed vulnerabilities across the security products for the past 15 years. As shown in the graph, the number of vulnerabilities discovered has been constantly decreasing from the year 2007; however in 2012 there was a sharp increase in the number of vulnerabilities.

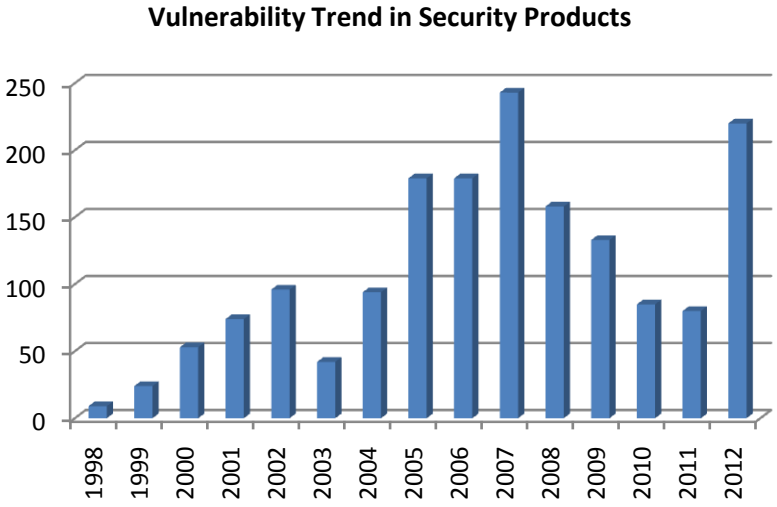


Figure 2: Shows vulnerability findings in security products. Y axis shows number of vulnerabilities discovered. X axis shows respective consecutive years.

©iViZ Security Inc 2013

Vulnerability Discovery in Major Security Product Types

Figure 3a & 3b shows vulnerabilities by percentage discovered in some of the major security product types over past 15 years and in 2012 alone respectively. As shown, Anti-Virus takes the lead followed up by Firewalls. Others security product types include Data Loss Prevention (DLP), Encryption, Backup, Secure Connection, Security Verification etc.

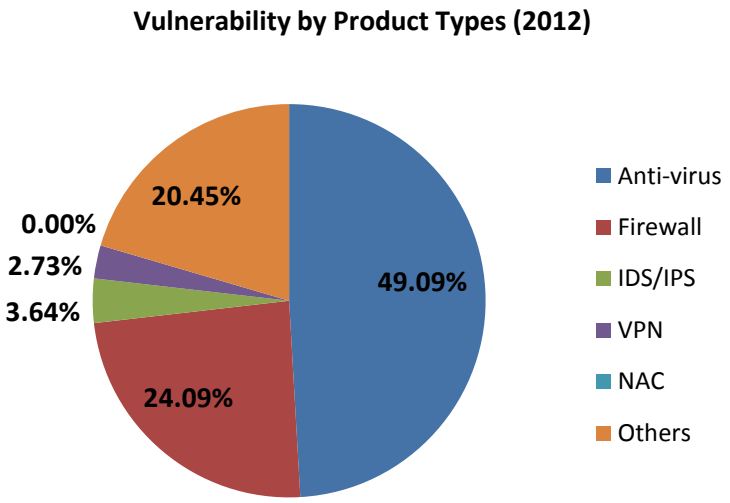


Figure 3a: Shows Vulnerabilities by percentage found against major security product types in 2012.

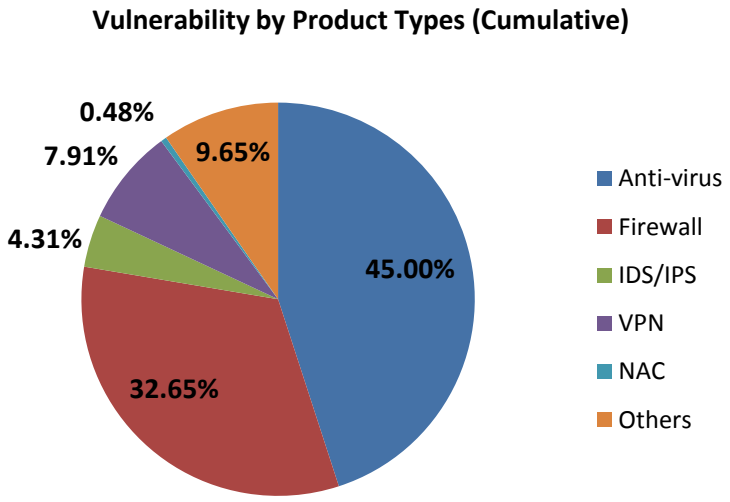


Figure 3b: Shows Vulnerabilities by percentage found against major security product types over the past 15 years.

©iViZ Security Inc 2013

Vulnerability Findings against Major Security Vendors

Figure 4a & 4b Shows the number of vulnerabilities discovered against some of the top security vendors over past 15 years and in 2012 alone respectively.

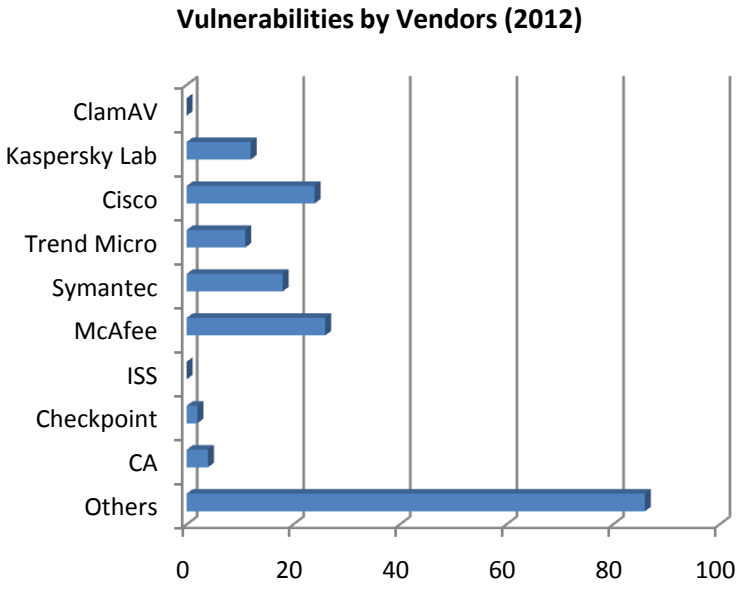


Figure 4a: Shows the number of vulnerabilities found against some of the major security vendors in 2012. X axis shows number of vulnerabilities. Y axis shows some of the major security vendors.

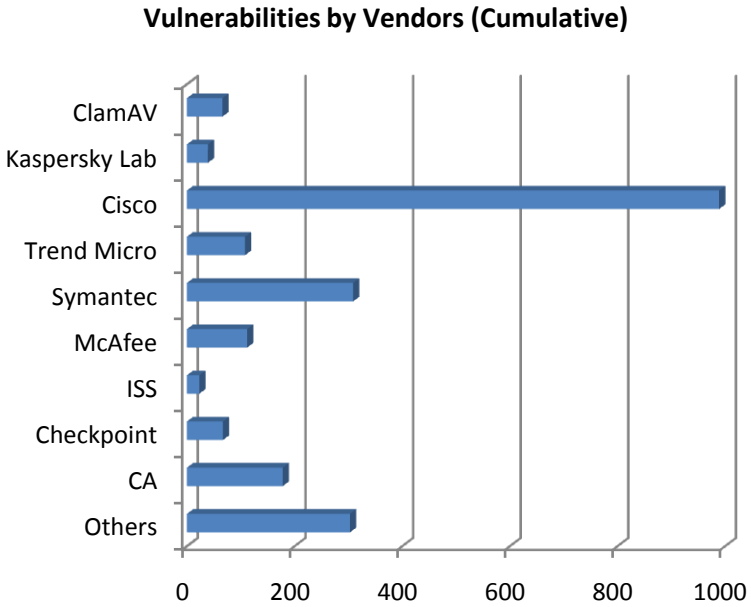


Figure 4b: Shows the number of vulnerabilities found against some of the major security vendors over past 15 years. X axis shows number of vulnerabilities. Y axis shows some of the major security vendors.

©iViZ Security Inc 2013

Vulnerability Findings in Major Security Products

Figure 5 Shows the number of vulnerabilities discovered in some of the major security products.

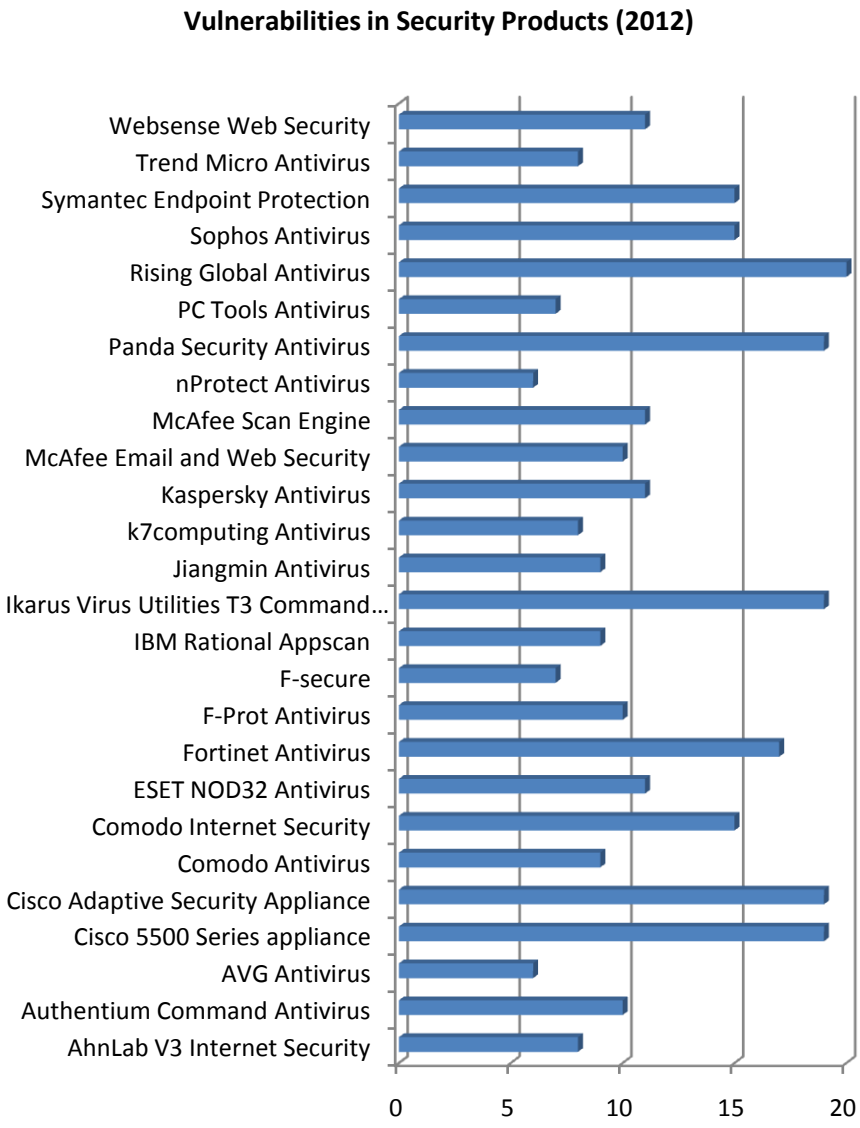


Figure 5: Shows vulnerabilities found in some of the major security products. X axis shows number of vulnerabilities. Y axis shows some of the major security products.

Security Weaknesses in Security Products

Figure 6 Shows the security weaknesses in all the security products. A security weakness is a flaw/bug in a product that gives rise to Security Vulnerability in the product. For the sake of comparison, we have also shown security weaknesses existing in the overall products existing today. As shown, SQL Injection weakness is less common in security products as compared to other non-security products. XSS Weakness is found to be the top weakness in 2012 for all products category which has replaced SQL Injection, which was top in 2011.Apart from SQL Injection, every other weakness is present in security

products as they are in all other non-security products. Probably, it shows that security products are subject to the same weaknesses and vulnerabilities as any other non-security products.

In security products, the two major weaknesses are Access Control and Input Validation and comparing with previous year there is a sharp increase in Access Control vulnerabilities.

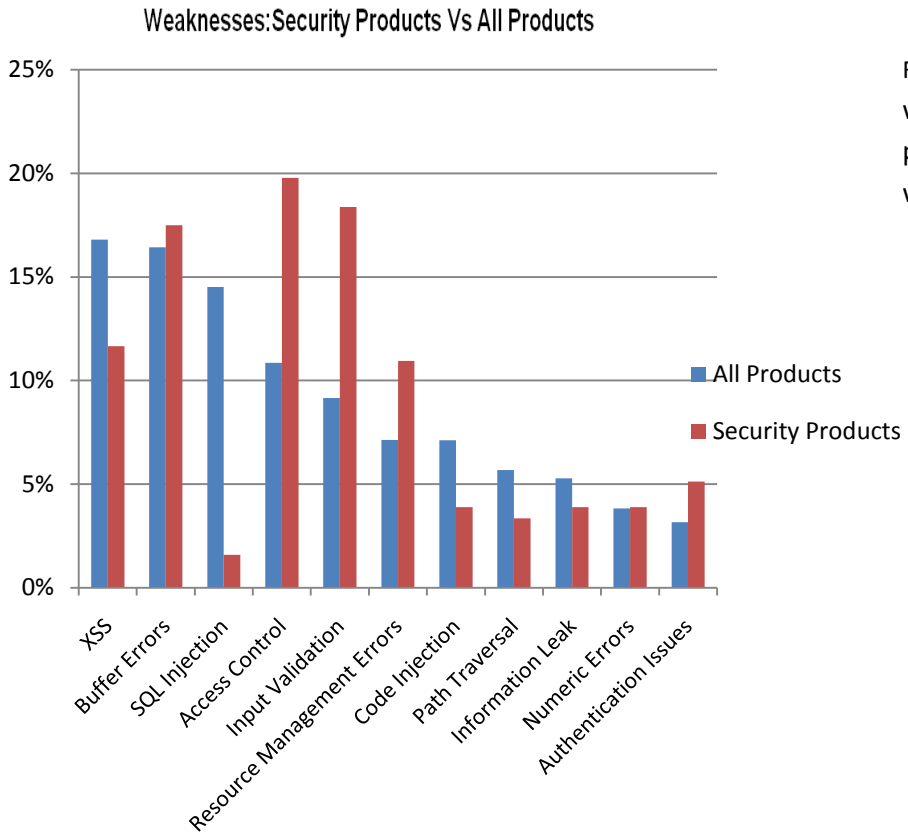


Figure 6: shows the weaknesses in security products in comparison with all products.

Conclusion

Here are the major trends which we foresee:

- There will be an increase in attacks on security products, companies or solutions.
- The majority of vulnerabilities discovered will not become public and shall remain in the hands of APT (Advanced Persistent Threat) actors.

As an industry we need to adopt more stringent measures in improving the security of security products. The following are a few steps which organization may adopt.

- Ask for security certifications of the products and independent third party penetration testing reports as part of procurement process.
- Conduct independent penetration testing of security infrastructure/solutions.
- Create an efficient detection and response mechanism.

References:

[1] GlobalCerts hacked, data leaked by #Anonymous
[2] Panda Security Hacked: Is Your Company's Website Safe?
[3] Symantec backtracks, admits own network hacked
[4] Hackers Hit Symantec, ImageShack, But Not PayPal
[5] Authentication giant VeriSign hacked repeatedly in 2010: by Reuters 2012
[6] Strategic Cyber Securityby Kenneth Geers
[7] Second Annual Cost of Cyber Crime Study – Ponemon Institute
[8] Global Risks 2012: by World Economic Forum 2012
[9] Cyber War Will Not Take Place:Thomas Rid, 2012
[10]90% of US Companies Hacked.

Disclaimer:

We have used well known vulnerability standards and database like Common Vulnerability Enumeration (CVE), Common Product Enumeration (CPE) and Nation Vulnerability Database (NVD). One of the major challenges we faced was in classifying the products into security and non-security products, as the current product standard (CPE) does not support it. We solved this challenge by learning that security products have certain keywords like, ' ID'virus', 'firewall'S ', ' IPS ', 'scan' etc