



Is Firewall and Antivirus Hacker's Best Friend?

Authors

Jitendra Chauhan
Head Product Development
Jitendra.chauhan@ivizsecurity.com

Rudra Kamal Sinha Roy
Head Product Management
rudra@ivizsecurity.com



©2010-2014 iViZ Techno Solutions Pvt Ltd

All rights reserved. No part of this whitepaper may be reproduced or transmitted in any form by any means graphic, electronic, or mechanical without permission in writing from the publisher.

The contents of this book reflect the author's views acquired through his experience in the field under discussion. The author is not engaged in rendering any legal professional service. The services of a professional person are recommended if legal advice or assistance is needed. The publisher or author disclaims any personal loss or liability caused by utilization of any information presented herein. For publication rights, please send a mail to rudra@ivizsecurity.com

Abstract

For the last ten years, thousands of vulnerabilities (security flaws) have been discovered in all major-commercial and opensource - products and software. In general, information security has become vital in protecting the interest of any individual and organization. Security products like anti-virus, firewalls, IDS/IPS and VPN have become of paramount importance to provide highest degree of confidentiality, availability and Integrity (CIA) to individuals and organizations. However, it is foolish to assume that security products are free from any vulnerability (security flaws). An attacker can exploit these security flaws in your anti-virus, for instance, to get access to your computer or network. In this article, we will **provide a summary of vulnerability findings in some of the major security products over the past few years.**

Are security products themselves secure?

Vulnerability is a weakness that allows an attacker to bring down your network or to get access to sensitive information like login / password, credit card etc; or even to get access to root account of a critical computer in the network. Thousands of vulnerabilities have been discovered for the past two decades in all the commercial and open source software/products. Figure 1 shows all the vulnerability findings for the last decade. As shown, hacker's community has grown from 1990's to present significantly. The year of 2005 witnessed a great increase in vulnerability findings, post which there was no looking back. Viruses, malwares, spam and security breaches are on the rise. As a result, various security products like anti-virus, firewalls, IDS/IPS, VPN, NAC and many other have been developed and launched in the market to implement 'best of the security' for the individual and organization.

Vulnerability Findings for last two decades

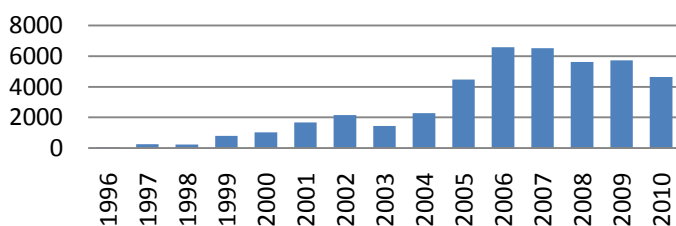


Figure 1: Shows vulnerability finding in all the known and documented products for past two decades. Y axis shows number of vulnerabilities discovered. X axis shows respective consecutive years.

In general, implementation of security can be divided into two major, complementary, approaches: *defensive and offensive*. Offensive security implementation requires performing ethical hacking (penetration testing) to find out security flaws in the network and applications, prioritize security flaws and finally provide recommendations to mitigate them. Defensive security requires installing various security products, processes and controls in the network. Security products include anti-virus, firewalls, IDS/IPS, VPN etc and are installed at various critical locations in the network to protect the network from attackers.

However these security products, themselves, are not free from vulnerabilities (security flaws) and can be the target of attacks from the intruders. In this article, a summary of vulnerability findings in the major security products has been presented. **Please note that we have neither targeted any individual**

company or product in this article nor do we say that any particular company or product is significantly more vulnerable than others. Our main objective, in this article is to highlight that security products, in general, are as vulnerable as any other products in your network. As a result, even the most secure of networks and applications require a more holistic approach, a mix of both defensive and offensive approaches.

History of Vulnerability Findings in Security Products

As shown in Figure 2, hackers have targeted security products to find significant number of vulnerabilities for the last ten years. All the major security products, anti-virus, firewalls, IDS/IPS etc have been found with security vulnerabilities. As with the overall trend (Figure 1), there was a significant increase in vulnerability finding from year of 2005.

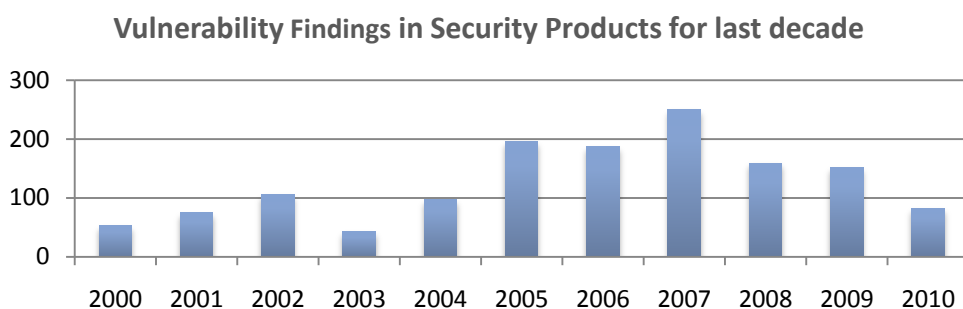


Figure 2: Shows historical data of vulnerability findings in security products. Y axis shows number of vulnerabilities. X axis shows respective years

Vulnerability Finding in Major Security Product Types

All major security products can be divided into security product types like Anti-virus, Firewalls, IDS/IPS, VPN, and others. Figure 3 shows the significant vulnerabilities that have been discovered in all these types of security products: Anti-virus seems to be the most affected products followed up by firewall products.

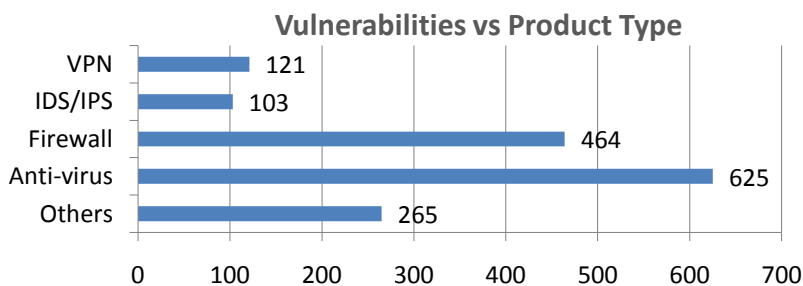


Figure 3: Shows vulnerability finding against major security product types. X axis shows number of vulnerabilities. Y axis shows major product types.

Vulnerability Findings against Major Security Vendors

Figure 4 shows vulnerability findings against some of the major security vendors: Cisco tops the list, followed up by Symantec. Is it that Cisco or Symantec products are more vulnerable than other security products in the market? The answer is no and it will be futile to interpret the data in this manner. Cisco and Symantec top the list simply because they have a larger number of products launched in the market. It is, however, definitely clear that security vulnerabilities can be found in products of even the major security companies of today and that no company can claim that they can create vulnerability free products.

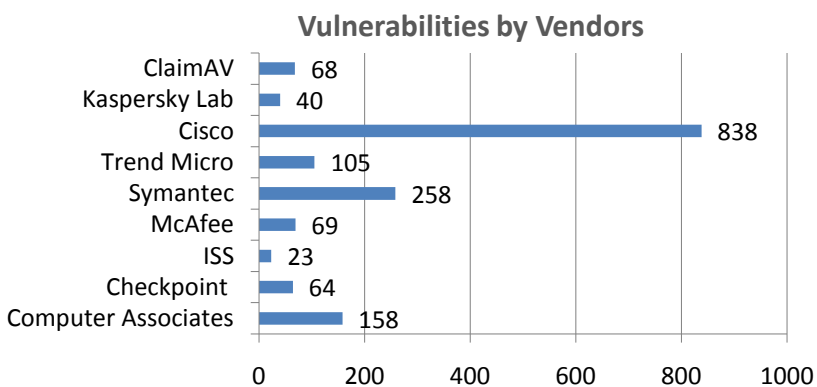


Figure 4: Shows the number of vulnerabilities found against some of the major security companies existing today. X axis display the number of vulnerabilities and Y axis display individual security vendors. Total vulnerabilities against each vendor are calculated by considering each individual product of the vendor and vulnerability finding in those products over the past years.

Vulnerability Findings in Major Security Products

Figure 5 shows vulnerabilities against some of the major security products existing today in the market. Please note that most of the security products are developed considering the best available development processes and practices by some of the most trusted vendors in the market.

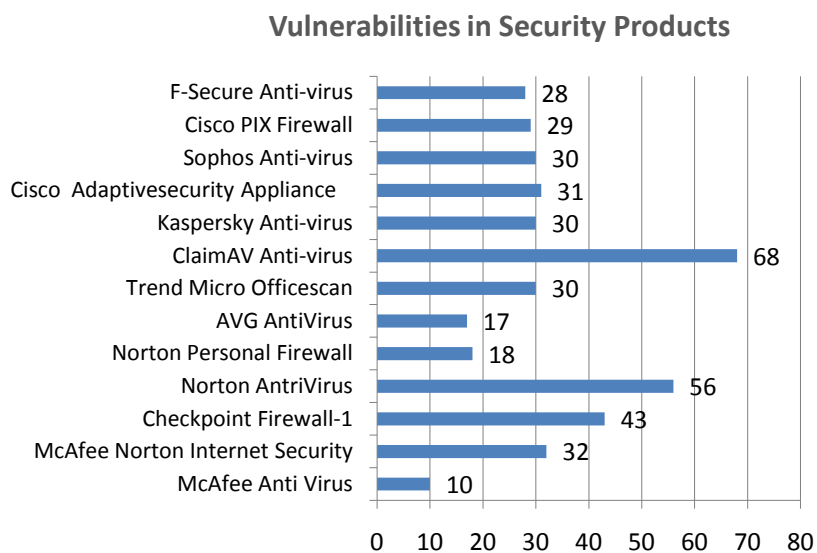


Figure 5: Shows number of vulnerabilities found in some of the major security products existing today. X axis display number of vulnerabilities and Y axis display some of the major security products. Total vulnerabilities against each security product are calculated by considering all the versions of the products and their individual vulnerabilities discovered over the past years.

Conclusion

Security products have been targeted by the hackers from the time they were introduced in the market. It should be noted that vulnerability findings in security products and software follow the similar trend as any other general purpose commercial or open source product.

Finally, it is worth noting some of the assumptions we took to compile the result. 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 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 'virus', 'firewall', 'IDS', 'IPS', 'scan' etc. Our statistics are also based upon vulnerability data latest by 5 Feb 2011; NVD updates its vulnerability database almost daily.

References

1. Common Vulnerability Enumeration (CVE): <http://cve.mitre.org/>
2. Common Product Enumeration (CPE): <http://cpe.mitre.org/>
3. National Vulnerability Database (NVD): <http://nvd.nist.gov/>
4. Common Weakness Enumeration (CWE): <http://cwe.mitre.org/>