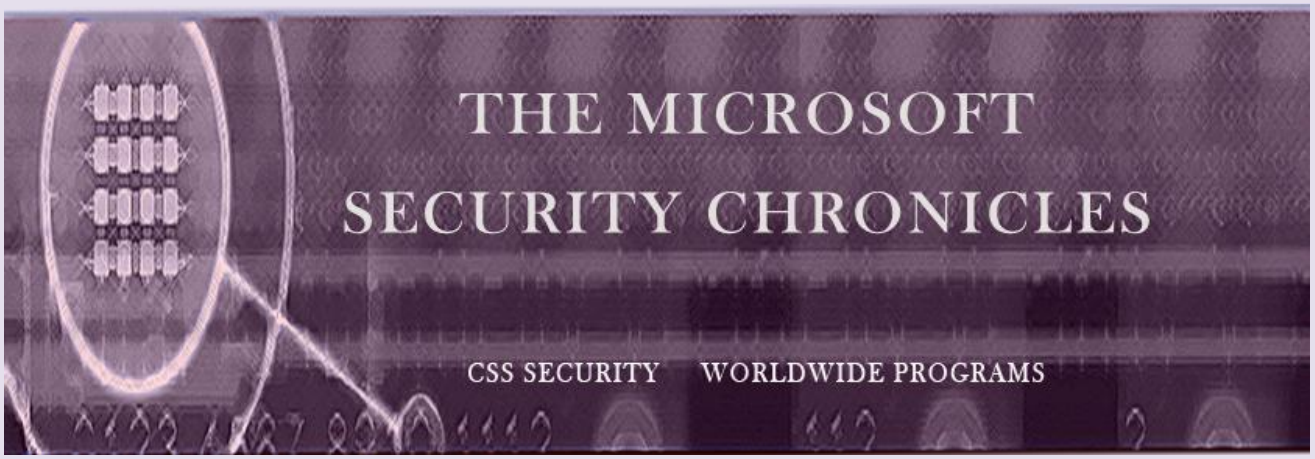


November 15, 2012

INSIDE THIS ISSUE

MICROSOFT RESOURCES

Microsoft Security Home

Microsoft Trustworthy Computing

Microsoft Security Sites Worldwide

Microsoft's Security Team Is Killing It: Not One Product on Kaspersky's Top 10 Vulnerabilities List

TNW

Microsoft products no longer feature among the Top 10 products with vulnerabilities. This is because the automatic updates mechanism has now been well developed in recent versions of Windows OS.

Analysis:

In case you were wondering - here are the top five products with vulnerabilities:

1. Oracle Java Multiple Vulnerabilities: DoS-attack (Gain access to a system and execute arbitrary code with local user privileges) and Cross-Site Scripting (Gain access to sensitive data). Highly Critical.
2. Oracle Java Three Vulnerabilities: Gain access to a system and execute arbitrary code with local user privileges. Extremely Critical.
3. Adobe Flash Player Multiple Vulnerabilities: Gain access to a system and execute arbitrary code with local user privileges. Gain access to sensitive data. Highly Critical.
4. Adobe Flash Player Multiple Vulnerabilities: Gain access to a system and execute arbitrary code with local user privileges. Bypass security systems. Highly Critical.
5. Adobe Reader/Acrobat Multiple Vulnerabilities: Gain access to a system and execute arbitrary code with local user privileges. Extremely Critical.

Ten years ago Microsoft got serious about security and launched the Trustworthy Computing group. Since that time Microsoft has expanded security into all of its operating systems and products. For instance, the Microsoft

SECURITY CALENDAR

November 2012

14 PacSec Tokyo

17 Kiwicon666 - Wellington

18 Global AppSec Latin America 2012 - Uruguay

27 DeepSec Vienna

28 Smart Card Alliance Government Conference – Washington, D.C.

December 2012

03 ASIS 6th Asia-Pacific Security Forum & Exhibition – Hong Kong

06 Microsoft Bulletin Advance Notification

10 WorldToor - Antarctica

11 Microsoft Security Bulletin Release

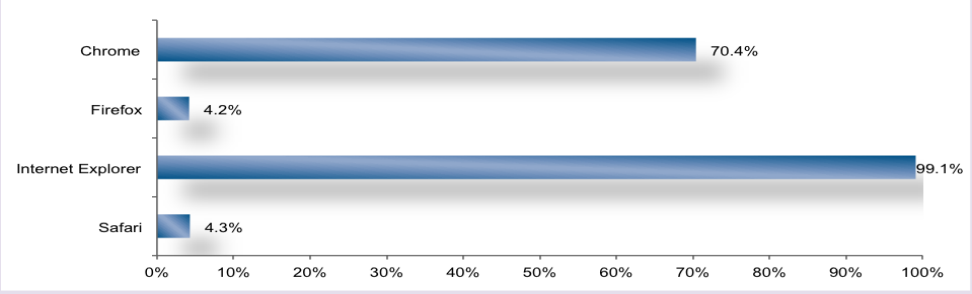
12 Blue Hat Redmond

Security Development Lifecycle is used worldwide and is shown to reduce security bugs.

Microsoft is committed to make sure its products are as secure as they can be as shown with the new Windows 8 operating system. This article talked about the great strides Microsoft has made in ensuring this new operating system is secure. "If you're using Windows and want to stay secure, get Windows 8. If you're not going to a third-party antimalware program on Windows 8, don't disable Windows Defender. Remember: No platform is 100 percent secure."

Microsoft also put a lot of work in Internet Explorer 10, which was analyzed in this article: Internet Explorer 10: The King of the Web Security. According to the latest study by NSS Labs, IE10 running on the Windows 8 protected test systems against 99.1 percent of all the malicious webpages, followed by Google's Chrome 70.4 percent mark. However, when it came to Firefox and Safari, the block rates were incredibly low, 4.2 percent and 4.3 percent respectively."

Overall Malware Block Rate by Browser (higher percentage is better)



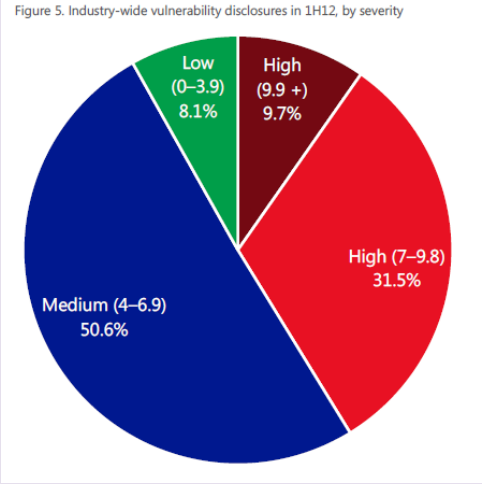
Source: NSS Labs

Microsoft also believes strongly in helping IT professionals and developers provide the most secure environments by providing tools and resources they can use. The Microsoft Technet Security Center is a wealth of information from Windows Server 2012 hardening to what threat determined adversaries and targeted attacks (PDF) pose.

Also for IT professionals Episode 22 on Technet is about SCM (Security Compliance Manager) 3 Beta. In this episode, Yuri Diogenes interviews Jose Maldonado, a senior program manager from Microsoft Solutions Accelerators Team – Security & Compliance. During this interview Maldonado talks about the Security Compliance Manager (SCM) 3.0 Beta. He explains what's new in this version, demonstrates how SCM 3.0 works and provides some information about Threats and Countermeasures documentation for Windows Server 2012 and Windows 8.

Microsoft's Trustworthy Computing Security group is also hard at work developing tools and processes to ensure our customers are more secure. They developed the Attack Surface Analyzer. This tool takes a snapshot of your system state before and after the installation of product(s) and displays the changes to a number of key elements of the Windows attack surface.

Microsoft also has a lot of great information in the Security Intelligence Report (PDF) that comes out twice a year. This latest volume contains information on deceptive downloads (software, music, and movies) and the worldwide threat assessment. The worldwide threat assessment goes into details on vulnerabilities, exploits, malware and potentially unwanted software, email threats, and malicious websites. Many of the charts contained are great reference material if you want to explain the current threat landscape. Here is a great example:



Source: Security Intelligence Report

As the threat landscape continues to grow, Microsoft is hard at work trying to ensure customers are protected. The Security Intelligence Report is definitely worth reading. Even if you can't read it cover to cover, there are some great takeaways, such as how to defend yourself against attacks. This provides enterprises as well as small businesses and consumers the ability to understand and implement security best practices.

The material in the Microsoft Security Chronicles is provided for informational purposes only. References to third party products, services or websites are provided only as a convenience to you and should not be considered an endorsement by Microsoft. Microsoft makes no warranties, express or implied, as to any third party products, services or websites. The views expressed in the linked articles are strictly those of the individual authors and/or publications.

©2012 Microsoft Corporation. All rights reserved. **Terms of Use** | **Privacy Statement** | **Microsoft Trademark List**