

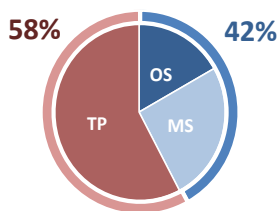
The average PC user in the USA has:

Programs Installed <h2>76</h2> <small>from 26 different vendors</small>	40% of these programs <h2>31 of 76</h2> <small>are Microsoft programs</small>	60% of these programs <h2>45 of 76</h2> <small>are from third-party vendors</small>	Users with unpatched Operating Systems <h2>21.1%</h2> <small>WinXP, Win7, Win8 Windows Vista</small>	Unpatched third-party programs on avg. PC <h2>10.5%</h2> <small>Unpatched MS programs: 3.5%</small>	End-of-Life programs on average PC <h2>3.8%</h2> <small>no longer patched by the vendor</small>
---	---	---	--	---	---

Introduction

This report documents the state of security among PC users in the USA, based on data from scans by the Secunia Personal Software Inspector, in Q4 2013. The security of a PC is largely controlled by the number and type of programs installed on it and to what extent these programs are patched. The data reflects the state of Secunia PSI users. It is safe to assume that Secunia PSI users are more secure than other PC users.

Origin of Vulnerabilities



Origin of vulnerabilities
Jan 2013 to Dec 2013

Operating System 17%
Microsoft Prog. 25%
3rd Party Prog. (TP) 58%

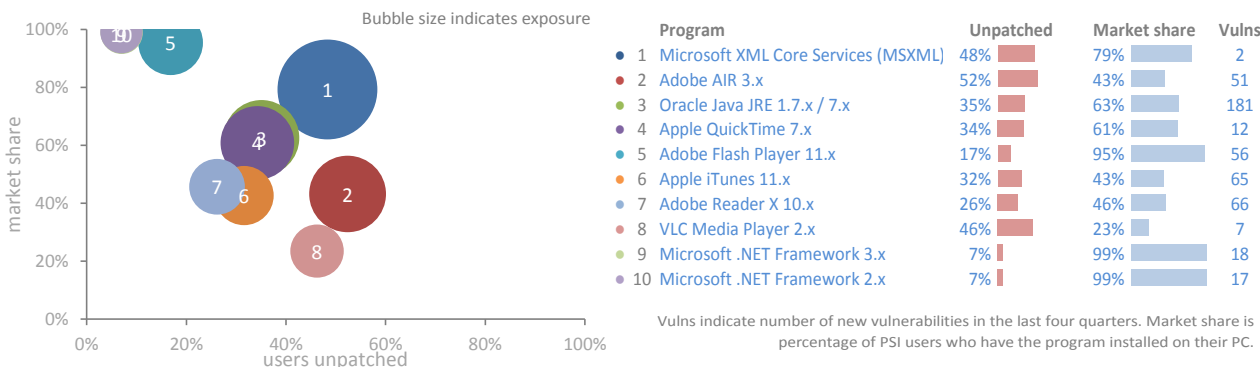
Cybercriminals know that most private users consider regular security maintenance of their PC hard work. As a result, a lot of users have PCs that are inadequately patched and therefore easily compromised.

On a typical PC, users have to master 26 different update mechanisms to patch the 76 programs on it, in order to remediate vulnerabilities:

- 1 single update mechanism for the 31 Microsoft programs that make up 40% of the programs on the PC.
- Another 25 different update mechanisms to patch the remaining 45 programs (60%) from the 25 so-called third-party vendors whose products are on the PC, and who each have a unique update mechanism.

Top 10 Most Exposed Programs

We have ranked the Top 10 of programs, based on risk exposure. We rank them based on 2 parameters: % market share multiplied by % of unpatched. That is, how widespread they are multiplied by how many of their users have neglected to patch them, even though a patch is available. The list at the far right shows how many vulnerabilities were detected for a program in the last four quarters (Jan 2013 to Dec 2013).



What does it mean?

If a vulnerable program remains unpatched on your PC, it means that your PC is vulnerable to being exploited by hackers. So if 35% of PCs running Oracle Java JRE 1.7.x / 7.x, who have a 63% market share, are unpatched, 22% of all PCs are made vulnerable by that program. The same PC can have several other unpatched, vulnerable programs installed.

Top 10 End-of-life (EOL) Programs

End-of-Life (EOL) programs are no longer maintained and supported by the vendor, and do not receive security updates. They are therefore treated as insecure. If you identify and remove End-of-Life programs you have made your PC a great deal more secure!

#	Program	Market share	#	Program	Market share
1	Google Chrome 30.x	37%	6	Microsoft Removal Tool: Blaster/Nachi	17%
2	Oracle Java JRE 1.6.x / 6.x	33%	7	Adobe Shockwave Player 11.x	15%
3	Mozilla Firefox 25.x	26%	8	Adobe Shockwave Player 10.x	13%
4	Mozilla Firefox 24.x	25%	9	Skype for Windows 5.x	12%
5	Adobe AIR 2.x	18%	10	OpenOffice.org 3.x	9%

Disclaimers

The data in this Country Report is a snapshot taken on 2013-12-31. Because Secunia Advisories are updated continuously, as new information becomes available, data in snapshots taken on different dates may vary.

Two different programs can have a shared code base and therefore share a vulnerability. This means that the same vulnerability will appear in 2 different programs. Therefore, when we group products the same vulnerability may be counted twice.

Remark

The percentage of unpatched users for a program/OS is highest shortly after the release of a patch

More Information

Secunia Personal Software Inspector (PSI) <http://secunia.com/psi>