

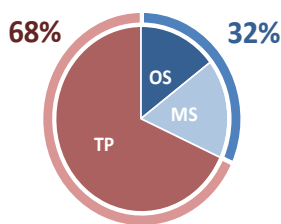
The average PC user in Denmark has:

Programs Installed <h2>69</h2> <small>from 22 different vendors</small>	39% of these programs <h2>27 of 69</h2> <small>are from Microsoft</small>	61% of these programs <h2>42 of 69</h2> <small>are from third-party vendors</small>	Users with unpatched Operating Systems <h2>7.5%</h2> <small>WinXP, Win7 Windows Vista</small>	Unpatched programs on average PC <h2>5.7%</h2> <small>3.1% Microsoft 7.6% 3rd party</small>	End-of-Life programs on average PC <h2>3.4%</h2> <small>no longer patched by the vendor</small>
---	---	---	---	---	---

Introduction

This report documents the state of security among PC users in Denmark, based on data from scans by the Secunia Personal Software Inspector, in Q1 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
Apr 2012 to Mar 2013

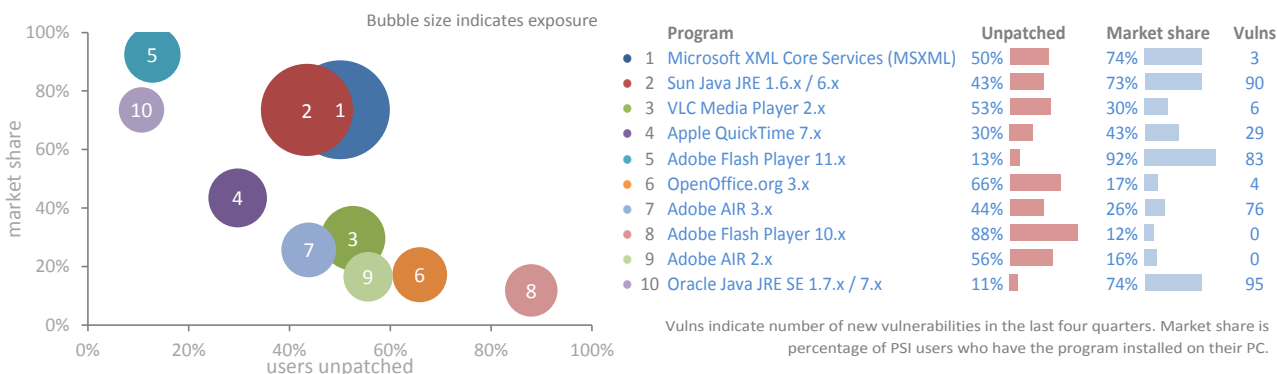
Cybercriminals know that most private users consider regular security maintenance of their PC hard work. As a result, a lot of users have PCs that are inadequately patched and therefore easily compromised.

On a typical PC, users have to master 22 different update mechanisms to patch the 69 programs on it, in order to remediate vulnerabilities:

- 1 single update mechanism for the 27 Microsoft programs that make up 39% of the programs on the PC.
- Another 21 different update mechanisms to patch the remaining 42 programs (61%) from the 21 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 certified vulnerabilities were detected for a program in the past year (Apr 2012 to Mar 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 53% of PCs running VLC Media Player 2.x, who have a 30% market share, are unpatched, 16% of all PCs are made vulnerable by VLC Media Player 2.x. 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 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	Microsoft Removal Tool: Blaster/Nachi	21%	6	RealPlayer 15.x	3%
2	Adobe Shockwave Player 10.x	15%	7	Media Player Classic 6.x	3%
3	Google Earth 5.x	5%	8	Sun Java JRE 1.5.x / 5.x	3%
4	Microsoft Office PowerPoint Viewer 2003	4%	9	CyberLink PowerStarter 6.x	2%
5	Adobe AIR 1.x	3%	10	Adobe Flash Player 9.x	2%

Disclaimer The data in this Country Report is a snapshot taken on 2013-05-21. Because Secunia Advisories are updated continuously, as new information becomes available.

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>