Australia

Secunia
Stay Secure

The average PC user in Australia has:

Programs Installed	40% of these programs	60% of these programs	Users with unpatched Operating Systems	Unpatched non-Microsoft programs	End-of-Life programs on average PC
81	**33 of 81**	**48 of 81**	**12.4%**	**11.6%**	**5.7%**
from 28 different vendors	are Microsoft programs	are from non-Microsoft vendors	Win7, Win8 Windows Vista	Unpatched MS programs: 4.5%	no longer patched by the vendor

Introduction

This report documents the state of security among PC users in Australia, based on data from scans by the Secunia Personal Software Inspector, in Q2 2015. 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

40%   **60%**

OS
NMS
MS
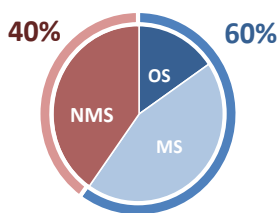
Origin of vulnerabilities
Jul 2014 to Jun 2015

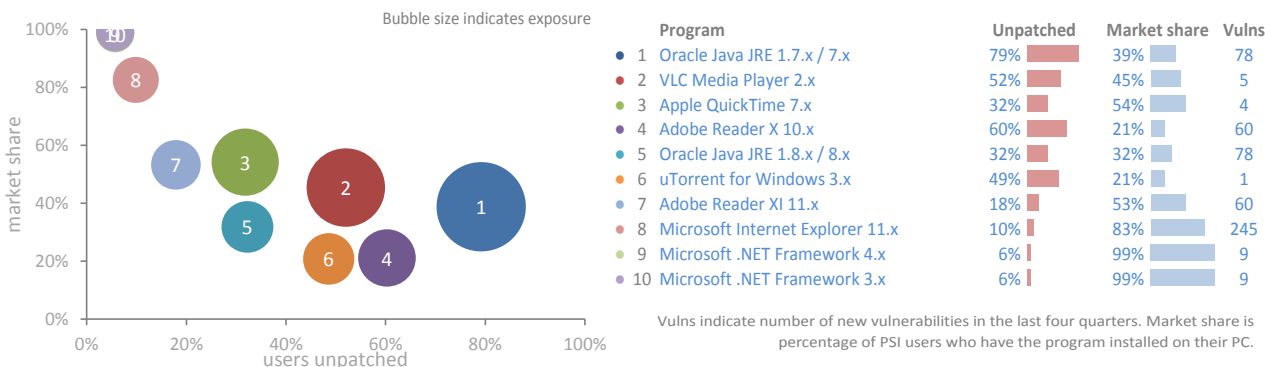| Operating System	15%
Microsoft Prog.	45%
Non-Microsoft Prog.	**40%**

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 28 different update mechanisms to patch the 81 programs on it, in order to remediate vulnerabilities:

• 1 single update mechanism for the 33 Microsoft programs that make up 40% of the programs on the PC.
• Another 27 different update mechanisms to patch the remaining 48 programs (60%) from the 27 non-Microsoft 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 (Jul 2014 to Jun 2015).

Bubble size indicates exposure

	Program	Unpatched	Market share	Vulns
1	Oracle Java JRE 1.7.x / 7.x	79%	39%	78
2	VLC Media Player 2.x	52%	45%	5
3	Apple QuickTime 7.x	32%	54%	4
4	Adobe Reader X 10.x	60%	21%	60
5	Oracle Java JRE 1.8.x / 8.x	32%	32%	78
6	uTorrent for Windows 3.x	49%	21%	1
7	Adobe Reader XI 11.x	18%	53%	60
8	Microsoft Internet Explorer 11.x	10%	83%	245
9	Microsoft .NET Framework 4.x	6%	99%	9
10	Microsoft .NET Framework 3.x	6%	99%	9

Vulns indicate number of new vulnerabilities in the last four quarters. Market share is percentage of PSI users who have the program installed on their PC.

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 32% of PCs running Apple QuickTime 7.x, who have a 54% market share, are unpatched, 17% 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	Adobe Flash Player 17.x	78%	6	Adobe Flash Player 16.x	20%
2	Microsoft XML Core Services (MSXML) 4.x	65%	7	Oracle Java JRE 1.6.x / 6.x	19%
3	Google Chrome 42.x	36%	8	Adobe AIR 17.x	14%
4	Mozilla Firefox 37.x	28%	9	Adobe AIR 3.x	12%
5	Google Chrome 41.x	22%	10	Apple iTunes 11.x	12%