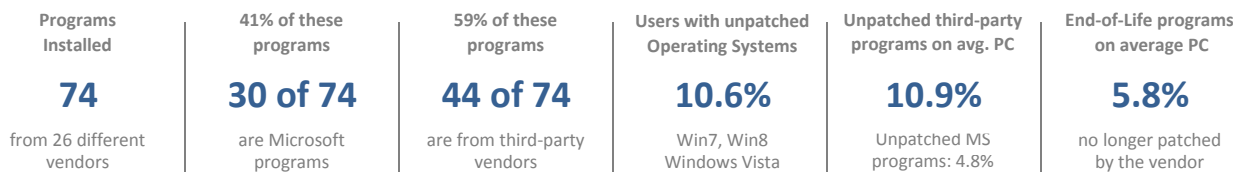


United Kingdom

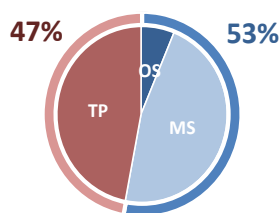
The average PC user in the United Kingdom has:



Introduction

This report documents the state of security among PC users in the United Kingdom, based on data from scans by the Secunia Personal Software Inspector, in Q4 2014. 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 2014 to Dec 2014

Operating System 6%
 Microsoft Prog. 47%
3rd Party Prog. (TP) 47%

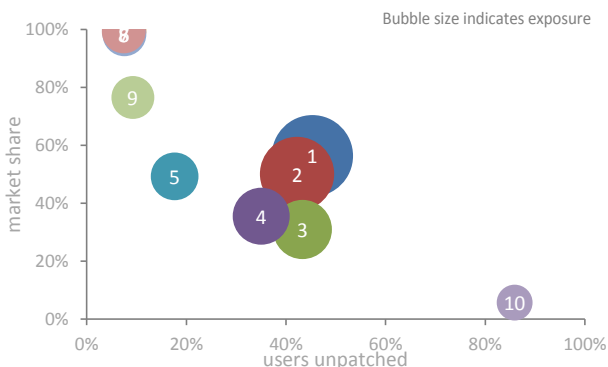
Cybercriminals know that most private users consider regular security maintenance of their PC hard work. As a result, a lot of users have PCs that are inadequately patched and therefore easily compromised.

On a typical PC, users have to master 26 different update mechanisms to patch the 74 programs on it, in order to remediate vulnerabilities:

- 1 single update mechanism for the 30 Microsoft programs that make up 41% of the programs on the PC.
- Another 25 different update mechanisms to patch the remaining 44 programs (59%) 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 2014 to Dec 2014).



Program	Unpatched	Market share	Vulns
1 Oracle Java JRE 1.7.x / 7.x	45%	56%	119
2 Apple QuickTime 7.x	42%	50%	14
3 Adobe Reader X 10.x	43%	31%	42
4 VLC Media Player 2.x	35%	35%	2
5 Adobe Reader XI 11.x	18%	49%	42
6 Microsoft .NET Framework 2.x	8%	100%	8
7 Microsoft .NET Framework 4.x	8%	98%	8
8 Microsoft .NET Framework 3.x	7%	99%	8
9 Microsoft Internet Explorer 11.x	9%	76%	248
10 Node.js 0.x	86%	6%	8

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 43% of PCs running Adobe Reader X 10.x, who have a 31% market share, are unpatched, 13% 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 15.x	79%	6 Google Chrome 37.x	23%
2 Microsoft XML Core Services (MSXML) 4.x	65%	7 Oracle Java JRE 1.6.x / 6.x	21%
3 Google Chrome 38.x	34%	8 Mozilla Firefox 32.x	18%
4 Apple iTunes 11.x	30%	9 Adobe AIR 3.x	16%
5 Mozilla Firefox 33.x	26%	10 Adobe Flash Player 11.x	11%

Disclaimers

The data in this Country Report is a snapshot taken on 2014-12-31. 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>