

# France

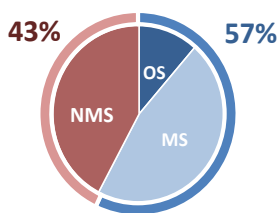
The average PC user in France has:

|   |   |   |  |  |   |
|---|---|---|--|--|---|
| <b>Programs Installed</b><br><b>79</b><br>from 29 different vendors | <b>37% of these programs</b><br><b>30 of 79</b><br>are Microsoft programs | <b>63% of these programs</b><br><b>49 of 79</b><br>are from non-Microsoft vendors | <b>Users with unpatched Operating Systems</b><br><b>10.1%</b><br>Win7, Win8<br>Windows Vista | <b>Unpatched non-Microsoft programs</b><br><b>12.2%</b><br>Unpatched MS programs: 4.9% | <b>End-of-Life programs on average PC</b><br><b>6.5%</b><br>no longer patched by the vendor |
|---|---|---|--|--|---|

## Introduction

This report documents the state of security among PC users in France, based on data from scans by the Secunia Personal Software Inspector, in Q1 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



**Origin of vulnerabilities**  
Apr 2014 to Mar 2015

**Operating System** 11%  
**Microsoft Prog.** 46%  
**Non-Microsoft Prog.** 43%

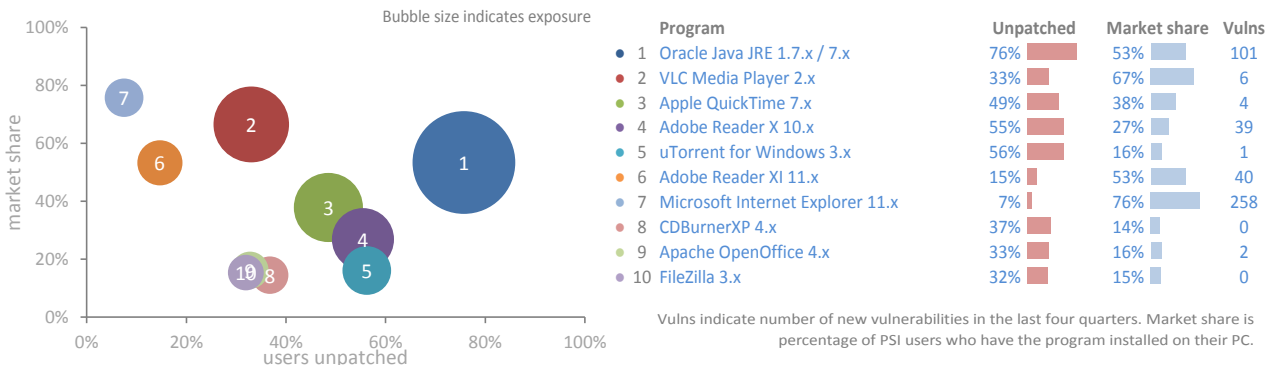
Cybercriminals know that most private users consider regular security maintenance of their PC hard work. As a result, a lot of users have PCs that are inadequately patched and therefore easily compromised.

On a typical PC, users have to master 29 different update mechanisms to patch the 79 programs on it, in order to remediate vulnerabilities:

- 1 single update mechanism for the 30 Microsoft programs that make up 37% of the programs on the PC.
- Another 28 different update mechanisms to patch the remaining 49 programs (63%) from the 28 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 (Apr 2014 to Mar 2015).



## 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 49% of PCs running Apple QuickTime 7.x, who have a 38% market share, are unpatched, 18% 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 16.x                 | 82%          | 6  | Oracle Java JRE 1.6.x / 6.x | 22%          |
| 2 | Microsoft XML Core Services (MSXML) 4.x | 72%          | 7  | Mozilla Firefox 34.x        | 18%          |
| 3 | Google Chrome 40.x                      | 45%          | 8  | WinRAR 3.x                  | 14%          |
| 4 | Mozilla Firefox 35.x                    | 36%          | 9  | OpenOffice.org 3.x          | 14%          |
| 5 | Google Chrome 39.x                      | 24%          | 10 | Adobe AIR 15.x              | 13%          |

### Disclaimers

The data in this Country Report is a snapshot taken on 2015-03-31. 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>