AN ALARMING TREND FOR END-USER SECURITY

To contribute to the debate on end-user security, Secunia carried out a dedicated study which looked at vulnerabilities affecting typical end-user PCs over five years[1]. We analysed the portfolio of the top-50 most prevalent programs found on typical end-user PCs, which consists of 26 Microsoft and 24 non-Microsoft (third-party) programs from 14 different vendors (including Microsoft). The number of vulnerabilities affecting this portfolio has increased at an alarming rate since 2007, and almost doubled to 420 vulnerabilities by 2009. In the first half of 2010 we reached 380 vulnerabilities, or 89% of the figures for the entire 2009. We expect the number of vulnerabilities affecting a typical end-user PC to almost double again by the end of 2010.

To better understand the threat, we divided the top-50 portfolio down into contributions from (A) the operating system, (B) Microsoft programs, and (C) from third-party (non-Microsoft) programs. This analysis clearly identifies vulnerabilities from third-party programs to be almost exclusively responsible for the increasing trend observed (see Figure 1). In 2009, a typical end-user PC with 50 programs installed had 3.5 times more vulnerabilities in the 24 third-party programs than in the 26 Microsoft programs. This ratio is expected to increase to 4.4 in 2010. This means a typical end-user can patch 35% of the vulnerabilities with one update mechanism (Microsoft's), but needs to master another 13 or more different update mechanisms to patch the remaining 65% of third-party program vulnerabilities.

Why end-user PCs?

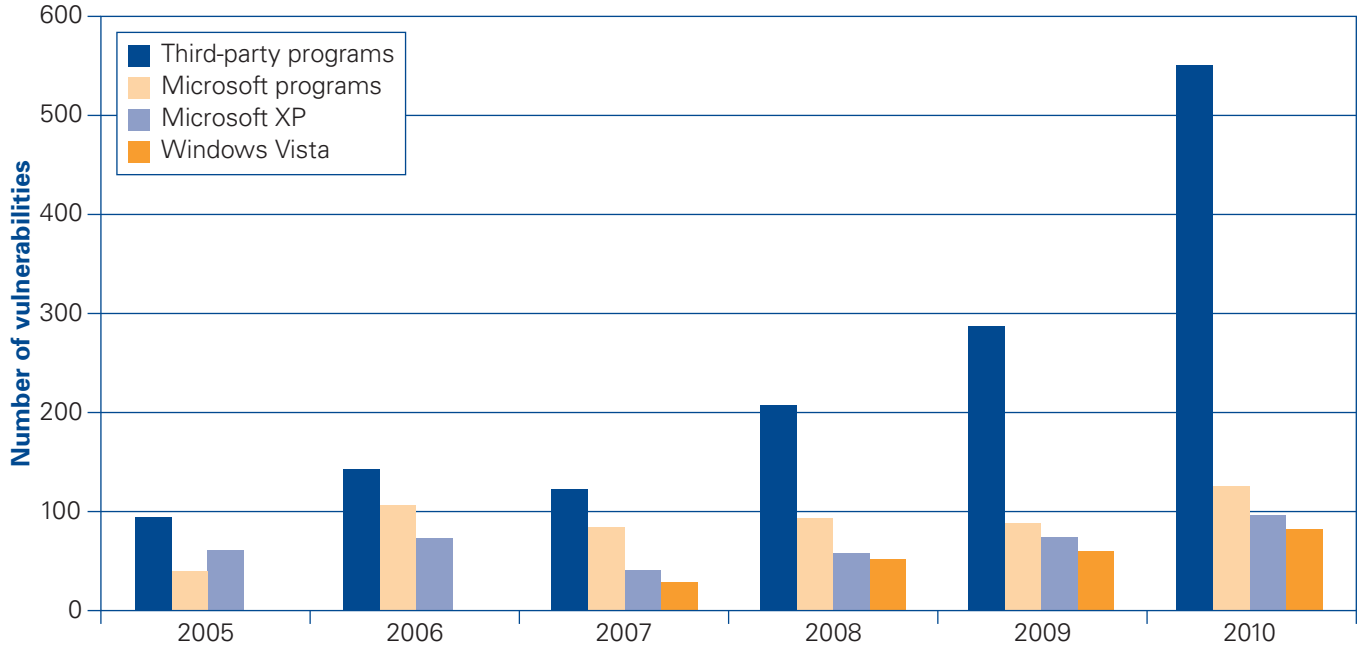
Vulnerabilities on end-user PCs are commonly exploited when the user visits a malicious/manipulated website, or opens documents with one of the numerous programs and

In 2009, a typical end-user PC with 50 programs installed had 3.5 times more vulnerabilities in the 24 third-party programs than in the 26 Microsoft programs. This ratio is expected to increase to 4.4 in 2010.

Secunia carried out a dedicated study which looked at vulnerabilities affecting typical end-user PCs over five years.

Stefan Frei reports

Figure 1: **Vulnerabilities in the operating system – Microsoft and third-party programs**



plug-ins installed on the PC. Recent research revealed that typically 50% of the users have more than 66 programs from more than 22 different vendors installed. The unpredictable usage patterns of users, and the variety and prevalence of programs found on typical end-user PCs, paired with the complexity of keeping programs patched using more than a dozen different update mechanisms, makes end-user PCs an attractive attack vector for cybercriminals. Only few vendors like Microsoft have the resources to implement an effective and easy to use auto-update mechanism. Focusing on third-party program exploitation therefore will continue to provide attackers with a large pool of commonly used software that is easy to exploit, and much less likely to be found fully patched.

Some of the reasons for businesses and private users not focusing on patching third-party programs are:

A) The perception of the operating system (OS) and Microsoft products being the primary attack vector
B) The frequency and complexity of managing a large number of different update mechanisms

Users and businesses must change their perception that Microsoft products pose the largest threat; general awareness on the risk of third-party programs must be established. An effective way to reduce the risk exposure is reducing the complexity in patching the variety of programs typically found on end-user PCs.

This would enable users to readily install patches, and thereby reduce the window of opportunity for criminals. Secunia is currently testing the free Personal Software Inspector (PSI) 2.0[2], which can automatically update a broad variety of programs from a number of different vendors.

A typical end-user can patch 35% of the vulnerabilities with one update mechanism (Microsoft's), but needs to master another 13 or more different update mechanisms to patch the remaining 65% of third-party program vulnerabilities.

Recent research revealed that typically 50% of the users have more than 66 programs from more than 22 different vendors installed.

It is our hope that Secunia PSI with auto updating will significantly improve the security of home users PCs. For businesses Secunia has developed the Corporate Software Inspector (CSI), an authenticated vulnerability and patch scanner that facilitates simplified patch management by integrating with Microsoft WSUS and SCCM, for both Microsoft and thousands of third-party programs. ■

[1] Secunia Half-Year Report 2010
http://secunia.com/gfx/pdf/Secunia_Half_Year_Report_2010.pdf
[2] Free Personal Software Inspector (PSI)
http://secunia.com/vulnerability_scanning/personal/

Stefan Frei is Research Analyst Director at Secunia.

www.secunia.com