Print This Article

<< Return to To be completely patched requires an average of between 51 and 86 actions per year

To be completely patched requires an average of between 51 and 86 actions per year

Dan Raywood
March 08 2010

An average of 75 patches from 22 different vendors needs to be installed every 4.8 days in order for the typical home user to stay fully patched.

In a blog update by Secunia CSO Thomas Kristensen, whose whitepaper 'Security Exposure of Software Portfolios' focuses on the problem, said that the findings are based on data from its Personal Software Inspector (PSI), and supports the fact that the complexity and frequency of actions required to keep a typical home user's system fully patched and secure, most likely exceeds what users are willing and able to invest.

The analysis in the whitepaper revealed that 90 per cent of users surveyed have to handle on average between 51 and 86 patch actions per year in order to address between 200 and 342 vulnerabilities affecting the programs of nine to 36 vendors in their software portfolios.

It said: "The complexity of the task to simply keep a home system up-to-date clearly shows the need for accurate vulnerability intelligence; and for tools to help identifying and patching all these programs.

"Our analysis demonstrates, that the total effort, and the frequency of actions, required to keep an end-user system secure most likely exceeds what the typical user is able, or willing, to invest into the security. As with back-ups, if the process is not fully automated and monitored, it is almost certain to fail when most needed – with dire consequences.

"Unlike back-ups, we still lack the technology, processes, or a common standard to facilitate the automated patching of diverse programs, across different vendors, at global scale. Major software vendors could afford the development and continued operation of state-of-the-art update processes. However, the increasing number of third party programs, plug-ins, and technologies creates new challenges.

"Given the increase in e-crime and the subsequent quest to find new ways to compromise end-user systems, it is no surprise that criminals have changed their primary focus from Microsoft programs to third party programs; and Adobe programs in particular due to the prevalence of these on end-user systems."

Microsoft last week confirmed that it will cover eight important vulnerabilities on its monthly Patch Tuesday tomorrow.

Kristensen said his company is just a few months away from releasing a free tool that will automate the installation of software updates for dozens of commonly installed third party programs. He said the tool will allow users to exclude certain applications, in the event that they do not want to automatically update specific programs.

Security blogger Brian Krebs said: “Such an application, if done right, broadly adopted, and not resisted by third-party software vendors, could well reduce the number of Windows users whose machines get trashed by drive-by downloads, as all of these malicious or hacked sites try to silently install malware by targeting security holes in third-party software, such as Flash and Adobe Reader.

“If I seem excited about the availability of a free meta-patching tool, it's probably partly for selfish reasons. Such a tool would almost certainly spell relief for anyone who is unlucky enough to be the appointed tech support guy for their family and friends, since fewer vulnerable applications means fewer compromised PCs, and hopefully less frequent pitiful pleas for help.”