



The H open source security

In association with heise online

You are a guest • Login | Register



Last 7 days News Archive Features Forums Newsletter RSS

 Search

4 May 2009, 15:14

« previous | next »

Study says silent updates enhance security

Updating browsers without first asking users is apparently the most successful way of ensuring wide distribution for the latest version – thus minimising the number of vulnerable browsers. A joint study by Google Switzerland and the ETH (Swiss Federal Institute of Technology) in Zurich concludes that, if an update requires too much user interaction or effort, users will either abort the process or fail even to run it.

Updating Opera requires a manual download and the subsequent installation involves several dialogues, so only 24 per cent of the users observed installed the latest version, says the study, but things are precisely the other way round with Google's Chrome: if an update is available, it's downloaded and installed without the user's being consulted ("silent update"). Twenty-one days after the provision of an update, 97 per cent of the Chrome users observed were using the current version. It isn't possible to disable automatic updating in Chrome anyway.

In the case of Firefox, 85 per cent of users were surfing with the latest version 21 days after its release, while the figure for Safari was 53 per cent. The researchers say their web servers were unable to make any measurements for Internet Explorer because it doesn't provide enough information about its patch state.

On the basis of their results, the authors of the study recommend that browser developers implement silent updates, given their obvious advantages. Opera at least is planning to introduce automatic updating for its coming version 10, but it probably still won't work without user involvement.

The authors also call for changes to patch strategies and patch cycles, pointing out that Microsoft's rigid monthly Patch Day is primarily an obeisance to its business clients, who require fixed times for updating their infrastructures. When there are critical vulnerabilities in Internet Explorer, however, they say it's hard to see why millions of other users should have to remain unprotected for a long time until the next Patch Day. Qualys, a provider of security services, [complained](#) in February about IE patches not being issued separately from other security updates, so that plugging holes took several weeks.

Although silent updates offer many users enormous advantages from a security point of view, they also involve a loss of control. Not every user may fancy having new and unrequested versions thrust on to the hard disk after an initial deliberate installation has been made. It also needs to be clarified whether silent updates ought to be restricted to security measures, or whether new functions might also be secretly incorporated into systems.

The complete study is available online as [Why Silent Updates Boost Security](#).

(djwm)

Add your comment

Print version | Send by email

« previous | next »

Share this article

Advertisement



Internet Toolkit

- Anti-Virus
- Browsercheck
- Emailcheck
- Conficker test
- Test SSL certificates
- Whois query
- My IP address
- Traceroute
- DNS query
- Subnet calculator
- MAC addresses
- RFCs
- Ping
- Bandwidth calculator
- Spam list query
- IP addresses



The H Security Conficker information site

The H Security information page on Conficker is where you can find the latest stand-alone removal tools, news, scanners and tips about the Conficker worm.

Simple Conficker test for end users

The H Security, in conjunction with heise Security, now offers a simple test that allows end users to check whether a system has been infected with Conficker version B or C

The right way to handle encryption with Firefox 3

Mozilla has changed the way Firefox 3 handles certificates, but not always for the better. A few modifications will sort things out - and give you more security



Open source Exchange replacements

The H takes a look at the open source alternatives to Microsoft Exchange Server messaging and groupware

Kernel Log: What's coming in 2.6.30 - File systems: New and revamped file systems

There are numerous changes affecting data security and Ext3 and Ext4 performance. EXOFS and NILFS2 and FS-Cache for AFS and NFS are all new. Although it is now barely maintained, there are also fixes for ReiserFS

Distributions: From Ubuntu to Mandriva and Fedora

This spring sees a burst of activity for Linux distributions. In addition to Ubuntu and Mandriva, FreeBSD and OpenBSD also put final touches on their new releases



Ubuntu 9.04 on the test bench

Ubuntu remains firmly entrenched at the top of the list of the most popular distributions. Version 9.04 (Jaunty Jackalope) includes various new features and many minor tweaks without modifying the established basic design

BullionVault.com - Gold with an open source soul

Gold and open source do not normally go together, but at BullionVault, the combination of both has created an innovative way of trading in the precious metal

With Oracle buying Sun what will become of

Linux Apache MySQL Perl

Klauser Informatik
- Ihr Partner für
Offene Systeme
www.klauser.ch

Ssl Encryption

Solutions for Your
Small Business
Business Begins
Here.
www.business.com

Patch Management

Agent and agent-less
Top ranked by
IDC
www.shavlik.com

Last Chaos MMORPG

Kostenloses 3D
Online Rollenspiel.
Jetzt erstmals
komplett in
deutsch!
LastChaos.gamigo.de/La