Important Apple security updates for Snow Leopard and Lion - get 'em today!

Blog Post from Paul Ducklin, Sophos

Hot on the heels of the iOS 5.1.1 release, Apple has pumped out a raft of security updates for Snow Leopard (OS X 10.6) and Lion (OS X 10.7) users.Here they are:

* OS X Lion 10.7.4.

The blurb is at DL1525; the 40,000-foot overview is at HT5167; and the all-important security details are at HT5281.

This update patches numerous vulnerabilities. These include issues at Bronze, Silver and Gold medal levels of insecurity.

There are vulnerabilities leading toinformation leakage (other people can look at data they're not supposed to see, up to and including raw passwords),escalation of privilege (non-admin users can get administrative access they're not supposed to have), and remote code execution (untrusted external content, such as a web page, can run software on your Mac without warning).

Notably, the 10.7.4 update fixes the recently-discovered FileVault flaw. Apple inadvertently shipped a version of FileVault - the software which seamlessly encrypts your home folder - with a debugging option turned on.

This caused OS X Lion to record your personal password in its log file, where others could retrieve it. Of course, passwords should never be stored in plaintext, so this was a monster-sized blunder.

* Security update 2012-002 for 10.6.8.

Once again, refer to HT5281 for details. This is Snow Leopard's equivalent of the 10.7.4 update.

(Some of the vulnerabilities listed in HT5281 apply only to Lion - such as the FileVault password logging fault. Some apply only to Snow Leopard. Many apply to both. Apple has chosen to document them in one place, for a total of 26 vulnerabilities patched in 19 system components.)

* Remote Desktop client update.

This patch is part of the OS X Lion point update to 10.7.4, but isn't included in the 2012-002 update pack for Snow Leopard users. So if you're on 10.6.8, you get this one separately.

* Safari 5.1.7.

This is nice! The notification is at DL1531 and some implementational detail is at HT5271. The security fixes - which include a patch for the remote code execution issue addressed two days ago in iOS 5.1.1 - are at HT5282.

New to Safari 5.1.7 is a feature which automatically turns off the Adobe Flash plugin inside your browser if it goes out of date.

When you update your Flash version - an update Apple's own processes obviously can't control - then the plugin gets reactivated.

If you really want to run with the outdated plugin, HT5271 tells you how.

But you really shouldn't. Plugins such as Flash and Java are vigorously analysed by crooks in the hope that they'll find a way to trick them into downloading program code without permission.

What more to say?

These updates should be considered either necessary (in the case of the security patches) or at the very high end of highly desirable (in the case of Safari 5.1.7).

Get 'em today!

PS. Just so you know: you will need to reboot in order to activate these updates.