

By: Filippo 2008 Apple News Editor

[Mega Security Update Released for Tiger and Leopard Users](#)

Update 2008 - 002 addresses issues that may enable a local user to execute arbitrary code with system privileges

Apple has just issued a new **security update for Mac OS X users**. The update has been made available for both Mac OS X 10.4.11 (**Tiger**) and Mac OS X 10.5.2 (**Leopard**) users. It addresses vulnerabilities that may lead to arbitrary code execution, or enable a local user to execute arbitrary code with system privileges. It is aimed at around 80 (most of which critical) issues. The must-perform update weighs in at around 104MB. "Security Update 2008-002 is recommended for all users and improves the security of Mac OS X. Previous security updates have been incorporated into this security update," says Apple. As usual, the Cupertino-based company doesn't offer specifics at first glance. Here's where you can see exactly how many aspects this security update addresses. However, just so you know, update 2008 - 002 mostly addresses issues with AFP, Apache, AppKit and CUPS. Help Viewer is also patched, as well as core networking features. The recent discovery of a [Mac OS security glitch](#) has triggered "threats" on behalf of Jacob Appelbaum and Adam Boileau (who've acknowledged the programming flaw), as a response to Apple's and Microsoft's non-response to the issue. The latter, who's known about the glitch as a Windows threat for quite some time, has already made the code available to exploit this vulnerability on his website, as a download. Appelbaum said he was prepping to do the same thing, him being "on Apple's side," but fed up with the lack of response to the issue on behalf of the Cupertino folks, as much as Boileau. Applebaum has given Apple three months to act, after which he promised to make the code available for download too. "This is a real problem and it needs to be fixed," said Jacob Appelbaum. He disagrees with the company's response saying "they won't put it in the latest security update or release a security update just for this issue." Jacob is a San Francisco-area programmer who discovered the vulnerability and reported it to Apple. [Apple](#) uses SHA-1 digests on Apple Featured Software so you can [verify](#) (with a high degree of probability) that the software you downloaded is the same software you intended to download (see Related documents below). When the SHA-1 digest for the file you downloaded matches the digest for the file as displayed on Apple Featured Software, you can be sure that the file is authentic. SHA-1 digest performs automatic verification for updates delivered by Automatic Software Update.