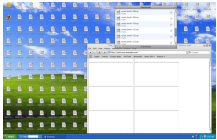


30 May 2008



This is what can happen to Windows users, according to Nitesh Dhanjani
Nitesh Dhanjani

By: Filip Truta, Apple News Editor

[More Voices Calling on Apple to Fix the Safari 'Carpet Bomb'](#)

Apple still short on a Safari patch

ZDNet is reporting that "the Google-backed StopBadware coalition has called on Apple to rethink its stance" on the Safari "carpet bomb" issue. Reported weeks ago by Nitesh Dhanjani, [the flaw](#) puts both Mac and Windows users at a serious security risk, according to voices on the Internet. Apple doesn't seem to be on the same level with everyone. "Malware downloaded to the user's desktop without the user's consent" is the primary issue researcher Nitesh Dhanjani encountered with Apple's standard web browser on Mac OS X 10.5 Leopard. Research has revealed that it is actually quite simple to use the browser and deploy malware on a user's computer. Still, Secunia rated the vulnerability as "less critical" at the time and [still does](#). Files downloaded by Safari to the Downloads folder on Mac OS, or to the desktop, on Windows, "create the potential for multiple files of unknown nature to mingle with legitimate downloads", StopBadware is reporting. Nitesh Dhanjani's example shows that Safari "cannot be configured to obtain the user's permission before it downloads a resource: assume that `http://malicious.example.com/cgi-bin/carpet_bomb.cgi` is the following: `#!/usr/bin/perl print "Content-type: blah/blah"`. Since Safari does not know how to render content-type of blah/blah, it will automatically start downloading `carpet_bomb.cgi` every time it is served." Now, here's Apple's response to that: "We can file that as an enhancement request for the Safari team. Please note that we are not treating this as a security issue, but a further measure to raise the bar against unwanted downloads. This will require a review with the Human Interface team. We want to set your expectations that this could take quite a while, if it ever gets incorporated." So, it should be clear to everyone that Apple's standard web browser on Leopard running machines doesn't bother to ask users for permission when downloading content from websites. Since Safari does not know how to render the content-type of a certain address, it will automatically start downloading the "carpet bomb" every time it is served. Needless to say, you should take extra caution downloading stuff you know little or nothing about, at least until Apple issues a patch.