

2 June 2008

By: Marius Oiaga, Technology News Editor

[Microsoft: Restrict the Use of Safari on XP SP3 and Vista SP1](#)

Because of the Safari Carpet Bomb

Safari
Apple

When it transitioned the default browser of Mac OS X to Windows, Apple wrapped it up in a "secure by default" marketing aura, aimed to give users of the Microsoft proprietary operating system a real taste of browser protection. It is precisely Safari's high security level the reason for which Microsoft is advising users of Windows XP Service Pack 3 and Windows Vista Service Pack 1 to steer clear of Apple's browser. "Restrict use of Safari as a web browser until an appropriate update is available from Microsoft and/or Apple," is the Redmond company's advice in relation to the Safari Carpet Bomb issue made public by security researcher [Nitesh Dhanjani](#). [Tim Rains](#), Product Manager in the Microsoft Malware Protection Center, has revealed that the Redmond giant is aware of "new public reports of a blended threat that allows remote code execution on all supported versions of Windows XP and Windows Vista when Apple's Safari web browser for Windows has been installed. Safari is not installed with Windows XP or Windows Vista by default: it must be installed independently or through the Apple Software Update application." Dhanjani's Safari Carpet Bomb describes a problem where Apple's browser does not request user permission before downloading a resource to the Windows Desktop. According to Dhanjani, a malicious website could download specially crafted files, malware included, directly to the default storage location without user consent. Apple was informed of the issue but stated that Safari downloading malware directly to the Windows Desktop without a say from the users is not a security vulnerability, and that the issue would be addressed as a feature enhancement against unwanted downloads. According to Microsoft, the Safari Carpet Bomb puts at risk users of Apple's browser when run on XP SP2 and SP3, XP x64 (with and without SP2), both 32-bit and 64-bit Vista RTM, and Vista SP1. The Redmond company's blended threat is related to scenarios where the Safari Carpet Bomb can be exploited via a vulnerability in its own browser, with Internet Explorer 6 and 7 being impacted. "Apple Safari can be used to pwn users with Internet Explorer installed. Well, basically this means that attackers can pwn Windows users who browse the web using Safari for Windows," informed security researcher [Avi Raff](#). "I've decided to work with Microsoft on this issue, because this combined attack also exploits an old vulnerability in Internet Explorer that I've already reported to them a long time ago. The root of this combined attack is Safari's "Carpet Bomb" vulnerability that was recently found by Nitesh Dhanjani." Rains explained that Microsoft is hard at work investigating reports of the blended threat, but failed to deliver any additional details about how Internet Explorer 6 and 7 are affected, or their role in actively exploiting the Safari Carpet Bomb issues. Still, it is clear that only users of the Safari browser on all the supported versions of XP and Vista are at risk. Since Safari fails to be as bulletproof as Apple claims, the best course of action is to stop using the browser entirely on Windows until either Microsoft or Apple are able to address the matter. "We've activated our Software Security Incident Response Process (SSIRP) and are working with our colleagues at Apple to investigate the issue. We have identified steps customers can take to protect themselves in the workaround section of the advisory. We are currently not aware of any attacks and are monitoring the issue and are working with our MSRA partners to help protect customers," Rains added.