

30 July 2008

By: Filip Truta, Apple News Editor

Safari
Apple

New Safari Flaw Acknowledged - Allows 'Cross-Site Cooking'

Exploiting the vulnerability allows an attacker to pre-set the victim's session ID

A Safari vulnerability filed under Common Vulnerability and Exposures identifier CVE-2008-3170 (under review) says that Apple's standard web browser can allow an attack when handling cookie files in country-level top-level domains, such as .co.uk and .com.au, according to InformationWeek. Basically, an attacker only has to exploit the vulnerability. Should he succeed, he could perform a session fixation attack, which allows him to pre-set the victim's session ID and to use the fixed session ID for whatever reasons come to mind (but all the wrong ones generally do). A Session Fixation Vulnerability in Web-based Applications is described as follows, according to Acros (Digital Security Lab): *In a session fixation attack, the attacker fixes the user's session ID before the user even logs into the target server, thereby eliminating the need to obtain the user's session ID afterwards. There are many ways for the attacker to perform a session fixation attack, depending on the session ID transport mechanism (URL arguments, hidden form fields, cookies) and the vulnerabilities available in the target system or its immediate environment.* [The paper](#) Acros has on the Fixation Vulnerability offers detailed information about exploiting vulnerable systems, and recommendations for protection against said session attacks. Also known as "cross-site cooking," this kind of attack might include tricking a user to log in through a malicious form, the InformationWeek report explains on. This includes: exploiting a cross-site scripting vulnerability or meta tag injection flaw, breaking into host in the target server's domain, and network traffic alteration. Microsoft and other security firms have reportedly singled out Apple's Safari for the abundance of security problems surfacing lately. Although attacks making use of this vulnerability have not been reported so far, the vulnerability has been acknowledged and is real. Apple now has to address this security issue.