

17 September 2008

By: Lucian Constantin, Web News Editor



Critical browsers
security issues
presentation canceled
WhiteHat Security

Critical Clickjacking Vulnerabilities Affecting All Browsers Being Kept Secret

After consulting with Adobe, two security researchers canceled their ground breaking clickjacking exploits presentation

Security researchers Jeremiah Grossman and Robert "RSnake" Hansen have been working on developing several proof of concept exploits based on clickjacking techniques that affect websites on all browser platforms. They intended to present them at the OWASP AppSec Conference in New York later this month; however, after collaborating with Adobe in regard to one of the exploits, they had a change of heart and postponed the demo as a more serious underlying flaw was discovered.

Clickjacking is not a new type of attack, but is somewhat surrounded in a shroud of mystery. The concept behind clickjacking is that through not so highly complex tools or advanced skills, one could hijack user mouse "clicks" and use them for questionable activities. A WhiteHat Security presentation overview notes some of the things that can be done with clickjacking - "generating affiliate advertising revenue from the Website traffic of others, trade stock using corporation information passively gleaned, inhibit the online purchase of sought after items creating artificial scarcity, and so much more." The problem with such activities is that they are considered "business logic flaws" rather than illegal, as they are not explicitly covered by any current laws.

All this makes clickjacking attacks very hard to track, monitor or detect. There is scarce information about prevention or how widespread they actually are and this is exactly the reason why Jeremiah Grossman and Robert "RSnake" Hansen developed the proof of concept exploits that were to be demonstrated at the OWASP conference. They were trying to raise awareness that these are serious issues that should be more actively monitored and discussed.

Jeremiah Grossman, founder and Chief Technology Officer of the WhiteHat Security company, [explains](#) on his blog what the three exploits were about and how they shared their research with Microsoft, Mozilla and Adobe in an attempt to practice responsible disclosure. While working on these exploits, they arrived to the conclusion that clickjacking is a problem that needs to be addressed by browser vendors rather than web developers, because these attacks are so generic that practically all web developers should patch their own websites, which is far from an applicable solution.

In this regard, they contacted Microsoft and Mozilla, but since one of their exploits was also making use of an Adobe product, they also presented their findings to Adobe's Product Security Incident Response Team (PSIRT). What the researchers didn't realize until later is that the attack technique used in their exploit was based on a critical security flaw in the Adobe product. "One Clickjacking PoC utilized an Adobe product with an attack technique they considered to be a critical issue, we just hadn't realized it, so we narrowly avoided 0-day'ing them!", notes Mr. Grossman.

At the same time, Robert Hansen, CEO and Founder of the SecTheory security firm and also member of many international security-related projects and organizations, [posted](#) on his own blog that they've "discussed the high level concern with both Microsoft and Mozilla and they concur independently that this is a tough problem with no easy solve in sight at the

moment." Since browser developers will be unlikely to come up with a complete and permanent fix very soon and instead they will deploy small patches in order to fix parts of the problem, Adobe requested for more time in order to patch their own product. The security researchers felt morally obligated to temporarily cancel the speech instead of going ahead with a heavily neutered version of it.

Both Jeremiah Grossman and Robert Hansen pointed out that this was a voluntary decision and that they were not forced in any way. "I must stress, this is not an evil "the man is trying to keep us hackers down" situation, a la Michael Lynn vs. Cisco, or Chris Paget vs. HID, or MIT vs. MBTA and so on," says Mr. Hansen. Mr. Grossman points out that "at this time just about everyone out there using the latest versions of Internet Explorer (including version 8) and Firefox 3 is affected. " He also claims that "the only fix is to disable browser scripting and plugins" and adds that he does "realize this doesn't give people much technical detail to go on, but it's the best [they] can do right now."

David Lenoë, Product Security Program Manager at Adobe, [posted](#) about this on the Adobe PSIRT blog noting that they "worked together with Robert and Jeremiah to assess the impact of this issue, and they [the researchers] determined that it was in [Adobe's] customers' best interest to refrain from making this issue public until Adobe and web browser vendors have a chance to provide a fix or fixes to [their] mutual customers".

Tom Brennan, Board Member & Chapter President at OWASP as well as TCM at WhiteHat Security, sees things a bit differently and he [noted](#) in an e-mail that he believes "a information security conference with industry peers from around the world IS the place to discuss/debate topics such as these and they should NOT be suppressed by anyone." He also added that "this is not the only security person that will be providing breaking research, however this is the 1st that has been told not to talk about it thus far".