Adobe plugs Flash webcam spy hole

October 22 2011, by Nancy Owano

(PhysOrg.com) -- Adobe engineers on Thursday fixed a vulnerability in its Flash software that could enable attackers to use a person's computer webcam or microphone feeds for spying on the person. Adobe made changes to an Adobe website page that controls Flash user's security settings. The fix did not require users to do anything more than stop shaking. A few days before the Adobe fix, Feross Aboukhadijeh, a Stanford University computer science student, had gone public with his announcement of the Adobe flaw.

He had been able to confirm a bug in the Flash player allowing the potential for such eavesdropping. Users who clicked on certain links could possibly let attackers access their Mac webcams and mics.

As far as his exploits could tell, the vulnerability showed up on Macs when using Firefox or Safari browsers. Aboukhadijeh went on to say he went public only after he had first reported the vulnerability to Adobe through the Stanford Security Lab but got no reply a few weeks earlier."I think it's worth sharing it with the world now, so that Adobe pays attention and fixes it more quickly."

What was troubling was that there were no popups or other user notifications informing him that the camera video had been activated and made accessible. In other words, eavesdropping could take place with neither the user's permission nor knowledge.Adobe contacted him soon after Aboukhadijeh published his findings in his public disclosure to say that they were working on it.

The discovery is an example of a 'clickjacking' hole--where people's webcams or microphones can be turned on without their knowledge. The Adobe flaw discovery follows a clickjacking alarm raised in 2008 by security researchers Jeremiah Grossman and Robert Hansen.

The technical term for clickjacking is user interface (UI) redressing. The trickster combines Web programming features with social engineering to entice users into initiating actions that they otherwise would not want to take.

While the discovery and subsequent fix might be seen as All's Well That Ends Well, one academic thinks this week's incident is troubling based on what he reads between the lines.

In announcing the fix, Adobe said it was aware of a report describing a clickjacking issue related to the Flash Player Settings Manager. "We have resolved the issue with a change to the Flash Player Settings Manager SWF file hosted on the Adobe website. No user action or Flash Player product update are required." No user action or update required? That comforter is what rattles Steven Bellovin, Professor of Computer Science at Columbia University.

"Code on a remote computer somewhere decides whether or not random web sites can spy on you," he blogged in CircleID. "it's simply wrong for a design to outsource a critical access control decision to a third party. My computer should decide what sites can turn on my camera and microphone, not one of Adobe's servers."

© 2011 PhysOrg.com

Citation: Adobe plugs Flash webcam spy hole (2011, October 22) retrieved 18 April 2024 from https://phys.org/news/2011-10-adobe-webcam-spy-hole.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.