When web sites rely on security holes

devblogs.microsoft.com/oldnewthing/20060112-15

January 12, 2006

Raymond Chen

Perhaps the biggest risk when making a change in the name of security is all the things that may have been relying on the previously-lax security settings. After all, disabling an insecure feature is easy. The hard part is disabling it while retaining compatibility with people who were relying on that feature. In the security investigations I've been involved with, perhaps the largest chunk of my time is spent trying to find a way to mitigate the security hole without breaking existing customers. (And it's the Line of Business scenario that is the biggest question mark.) Here's a real-life example: Consider a sports web site which sells a service to subscribers wherein the site creates a pop-up window whenever a game's score has changed or some other significant event has occurred. That way, you can leave your browser minimized and go about your day, but when something happens in the game, it will pop up an alert. The round of security changes in Windows XP SP2 broke this site because the rules on positioning of pop-up windows were tightened so that pop-up windows could not appear outside the browser itself. This prevents pop-up windows from being used to cover important browser elements (such as the status bar, the address bar, or a security dialog) and makes it harder for pop-ups to masquerade as system dialogs. But it also broke this company's business model. And of course, if Microsoft does something that cause you to lose money, you sue. There were probably corporations that had internal web sites that relied on the ability to position pop-ups without restriction. Those corporations no doubt also complained about this change in the name of security.

As with most security changes that have compatibility consequences, a "safety valve" was added to return to the old insecure behavior for those customers who were relying on it. In this case, you can put the affected sites in the Trusted Sites zone and enable the "Allow script-initiated windows without size or position constraints" setting. But this is just a stop-gap, re-opening the security hole to let this site continue to operate the way it does. The real fix is not to rely on the security hole.

Raymond Chen

Follow