

Re: [Full-Disclosure] Gmail anomaly

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-11/0873.html>

From: Daniel Veditz (dveditz_at_cruzio.com)

Date: 11/19/04

Date: Fri, 19 Nov 2004 09:08:43 -0800

ifconfig_xl0 wrote:

- > *If you open two gmail accounts in two different firebird/fox browsers*
- > *the first account logged into after a refresh becomes the second*
- > *account. Or if you send an e-mail with the second account, it may*
- > *send as the first and refresh back as account1.*
- >
- > *So if you login with GmailAccount1 and then open another browser and*
- > *log into GA2, go back to GA1 browser and hit refresh, GA1 will be in*
- > *the mailbox of GA2.*
- >
- > *This obviously is not a security risk because the mailbox was already*
- > *logged into, but I still thought it was a weird thing to do. It doesnt*
- > *act that way with internet exploder though so it must be something*
- > *with Firefox ...*

In Firefox there is only ever one instance of the executable, and all windows share session cookies (and http auth, which has similar differences between IE and Firefox).

You get the same behavior from IE if you open new windows from existing browser windows (crucial for web apps to work). You get a new process that does not share session information if you launch a new window from the OS (Desktop link, start menu, command-line, etc).

In practice the difference doesn't matter to the average user, but there are lots of Bugzilla duplicates filed by power users asking Mozilla to mimic the IE behavior.

It becomes a minor security problem in conjunction with sites that assume the IE behavior and which lazily instruct the user to "close the browser window" to completely log out rather than reset the session info from the server side. This is insufficient even for IE if the user opens multiple windows using Ctrl+N or the File|New menu item.

-Dan Veditz

Full-Disclosure - We believe in it.

Re: [Full-Disclosure] Gmail anomaly

Full-Disclosure: Re: [Full-Disclosure] Gmail anomaly

Charter: <http://lists.netsys.com/full-disclosure-charter.html>