ColdFusion email security Bug: Your mail in the wrong sent folder?

Posted At : August 21, 2013 5:00 PM | Posted By : Mark Kruger
Related Categories: ColdFusion

A recent conversation on CF-Talk piqued my interest. It turns out there is a tricky bug with regard to sending authenticated mail. Here at CF Webtools we have internal relays (protected, internal only IPs, listed in SPF and handling domain keys) whose sole purpose is to relay mail from our web servers - so we do not have "authenticated" email per se. But in the case of this bug (you can see the report here) it's possible for email from one user to wind up in the "Sent" folder of email from an entirely different user. Needless to say this is a security concern for those of you on shared servers especially.

Here are the conditions that need to be met for this to occur (as I understand it).

- Server needs to be busy enough to be sending quite a bit.
- Mail server handling the outgoing mail must do more than just relay the mail. It must put the mail relayed into the "sent" folder of the authenticated user. That's not a common behavior for most mail servers. In this case Google Apps Gmail fits the bill. In my experience *most* mail servers do *not* do this. Indeed, I suspect that the bug was really introduced by this "feature" of Gmail (or perhaps other mail servers).
- The ColdFusion Administrator setting for "Maintain connection to mail server" (on the "mail" settings page) must be *checked*.
- Mail must be sent:
  - By multiple users on the server using SMTP authentication (i.e. the username and password of their account needed to relay)
  - Sending to the *same domain*

Complicated? Not really. Let's think about it for a moment. Bob sends an email to his mom using smtp.gmail.com with a user name of *bob@gmail.com* and a password of *pooky*. Bob's girlfriend Mary sends an email to *her* mom explaining what a dufus Bob is. She sends her message to smtp.gmail.com with a username of *mary@gmail.com* and a password of *sugarbear* (I think Bob and Mary are made for each other).

Bob's message arrives at CF, which creates a connection and sends the mail. Meanwhile Mary's message arrives right behind it. ColdFusion, which has been instructed to maintain and reuse connections, thinks to itself, "Hmmmm... I already have an open connection to smtp.gmail.com," and quick as a flash it sends Mary's email right behind Bob's down the same pipe.

But since Bob's connection was created with *Bob's* authentication properties this second email is placed in Bob's "sent" folder along with his own legitimate sent message requesting his Mom's recipe for cranberry chutney. The result? Bob see's Mary's email, learns that he is in fact a dufus as his father always claimed, collapses in tears, and a budding relationship is ended. I ask you - is it right for ColdFusion to rain on their emotional parade? Everyone needs someone right? Napoleon had his Josephine, Nicholas his Alexandra and of course Sonny had his share.

Anyway this is clearly a bug for 2 reasons. First, I sort of expect "maintain connections" to be a setting that affects the server I enter on the admin page (the default relay) - not *every possible* server a developer might specify. Second, it's clear to me that the authentication portion of an outgoing email connection is (or should be) something that uniquely tracks that connection. So a connection with one set of credentials should *not* match a connection with another set.

In any case this has some implications if your code meets the criteria above so make sure and handle it accordingly. Note, this affects ColdFusion 9 and 10 as I understand it.