Contact Us Form - Email Injection Attack

Posted At : September 5, 2005 4:27 PM | Posted By : Mark Kruger
Related Categories: Coldfusion Security

In the last few weeks I've noticed a new attack making the rounds on my CF server. Although it's not an effective attack against a CF server, it does illustrate how spammers are a boil on the butt of humanity. It's called "email injection" and it's actually an attempt to leverage a PHP vulnerability (or perhaps I should say a “bad PHP coding” vulnerability). How do you know if you are being attacked? If you have a web site with a "contact us" form or any other form whose result is a sent email, and you are getting emails "from" your own domain and "to" your own domain - using bogus email addresses you are probably seeing this technique in action. You will also get bounces and if you look in the raw bounce code you will see something like "bcc: *some email address*". That's the tip off. Please note, this technique does NOT work against Coldfusion as far as I know - only PHP seems to be referenced in the various online discussions of the topic. If you are interested read on.

Email injection is an attempt to exploit the file format of an email message. If you've ever looked in the spooler directory of your CF server or had the occasion to examine raw message formats on a mail server you will know that an email is really a file with instructions for delivery. There are a few required parameters (headers) and a number of optional ones. A typical mail message looks like this:

```
To: bob@cheetamsGarage.com
Subject: Car inquiry
From: agitated@customer.com

Bob,
Hey you deadbeat - when's my car going to be ready??
```

Of course, there's much more to it than that. There are a myriad of required and optional headers that are inserted into the message. These options and headers are interpreted by email clients, servers and other processes. Here's an example of an actual message - with the names changed to protect the less guilty.

```
From: bob@cheetamsGarage.com
To: agitated@customer.com
Subject: Your lousy car is done
Date: Wed, 6 Jul 2005 16:15:28 -0500
Message-ID: <MLEIJGOCGEICCNCMLCDCEEPBFFAB.cheetamsGarage.com>
MIME-Version: 1.0
Content-Type: multipart/alternative;
   boundary="----=_NextPart_000_016C_01C58245.EC77DDC0"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.6604 (9.0.2911.0)
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180
Importance: Normal

This is a multi-part message in MIME format.

------=_NextPart_000_016C_01C58245.EC77DDC0
Content-Type: text/plain;
   charset="iso-8859-1"
```

```
Content-Transfer-Encoding: 7bit

Dear Customer,


------=_NextPart_000_016C_01C58245.EC77DDC0
Content-Type: text/html;
   charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"> <HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =
charset=3Diso-8859-1">
<META content=3D"MSHTML 6.00.2900.2668" name=3DGENERATOR></HEAD>
<BODY>
<h4>dear customers</h4>
</body>
</html>
------=_NextPart_000_016C_01C58245.EC77DDC0--
```

As you can see the format can be pretty loose - with lots of stuff in there that may or may not belong - and the message can usually still be delivered.

How the Attack is Accomplished

PHP handles email through an email script. Such a script typically builds this file on the fly from the various inputs. As you can see the "linebreak" is the chief delimiter in the file format. If a user added a linebreak to the "subject" parameter, and then added a bcc header (for example) the output might end up looking like this:

```
To: bob@cheetamsGarage.com
Subject: Car inquiry
Bcc: target@nothappy.xxx
from: agitated@customer.com

....
```

You can see how that might make a bottom feeding spammer salivate. He can send spam messages *from you* to his victims through your own secure relay. That's sneaky and underhanded - which is why they love it I'm sure.

Additional Options

It get's worse than that. Using this methodology spammers can overwrite the subject, include HTML in the message and obscure text that is intended for the message. This post is one of the best explanations I found (actually more of a how to). It has a much more in-depth discussion of the issue and lots of PHP code samples

Coldfusion Implications

As far as I can see there are no CF implications. CF is in control of the file format sent to the spooler. It clearly defines the sections and headers and I doubt seriously that any attack could be constructed that would work against CF in this case. Please note, I have not tested it - I'm only making an educated guess. If the the attacks against the contact forms on my own site are any indication, we will know for sure very shortly. If you have some information on this subject *please* enlighten us.

follow up

There is a follow up post to this topic.