

Exploiting Google MX servers as Open SMTP Relays

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-05/msg00094.html>

- *From:* pablo.ximenes@xxxxxxx
 - *Date:* 7 May 2008 20:37:46 -0000
-

Vulnerability Report:

As part of our recent work on the trust hierarchy that exists among email providers throughout the Internet, we have uncovered a serious security flaw in Ggoogle's free email service, Gmail. This vulnerability exposes Google's email servers in a way that allows an attacker to use them as open spam and phishing relays. This issue is related to the risk of a malicious user abusing Gmail's email forwarding functionality. This is possible because Gmail's email forwarding functionality does not impose proper security restrictions during its setup process and can be easily subverted. By exploiting this problem an attacker can send unlimited spam and phishing (i.e. forged) email messages that are delivered by Google's very own SMTP servers. Since the messages are delivered by Google's own servers, an attack based on this flaw is able to bypass all spam filters that are based on the blacklist / whitelist concept. We were able to confirm that this vulnerability is indeed exploitable b

y crafting a proof of concept attack that allowed us to send any number of forged email messages without restriction through Google's server infrastructure. We have also verified that this flaw allows attackers to bypass spam filters by using our method to send messages that are usually flagged as spam. While sending these messages directly from our network in the traditional way had the messages classified as spam, by sending the very same messages using our exploit, the messages were delivered directly to the victim's inbox, thus bypassing filters.

Impact:

All email providers that offer Google's SMTP servers any special level of trust (e.g. whitelist status) are vulnerable.

Disclosure:

We have contacted Google about this issue and are waiting for their position before releasing further details.

For more information, visit our homepage:

<http://ece.uprm.edu/~andre/insert>

Regards,

Pablo Ximenes, André dos Santos

INSERT – Information Security Research Team

Exploiting Google MX servers as Open SMTP Relays

University of PR at Mayaguez (UPRM), USA
State University of Ceará (UECE), Brazil

pablo.ximenes@xxxxxxx, andre@xxxxxxxxxxxxxx