

[UNIX] Unfortunate Interaction Between EZMLM and MessageLabs Virus Scanning

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0056.html>

From: support@securiteam.com

Date: 05/12/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 12 May 2002 14:44:01 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Unfortunate Interaction Between EZMLM and MessageLabs Virus Scanning

SUMMARY

The widely used mailing list manager, <<http://cr.yip.to/ezmlm.html>> EZMLM, when sending mails for moderation, sets a reply-to address which, if responded to, will cause the mail to be accepted for distribution.

<<http://www.messagelabs.com/>> MessageLabs offer an email virus scanning service which, unfortunately, sends virus alerts to, amongst others, the reply-to address.

This causes email-bearing viruses to be automatically accepted even when sent to a moderated list.

DETAILS

A security vulnerability in the way EZMLM interacts with MessageLabs allows incoming viruses' detection message (that is sent to the author of the email) to cause EZMLM to allow through the incoming virus. This is caused by the way both product handle the Reply-To address, where one uses it for Moderation purposes (EZMLM) and another for virus infection notification (MessageLabs).

ADDITIONAL INFORMATION

The information has been provided by <mailto:ben@algroup.co.uk> Ben Laurie.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- *Previous message:* support@securiteam.com: "[TOOL] LSAT, Linux Security Auditing Tool"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)