

[NEWS] AeroMail Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0033.html>

From: support@securiteam.com

Date: 03/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 8 Mar 2002 11:23:12 +0100 (CET)

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.

AeroMail Multiple Vulnerabilities

SUMMARY

<<http://the.cushman.net/projects/aeromail/>> AeroMail is a web-based e-mail client written entirely in PHP using PHP's built in IMAP functions.

DETAILS

Vulnerable systems:

AeroMail versions prior to 1.45

Immune systems:

AeroMail version 1.45

Problem #1

When sending e-mails, you can trick the attachment subsystem into sending local files from the web server or remote files from URL's instead of uploaded files as it should.

How is that possible? Well, after PHP has uploaded a file, it sets a few variables with information about it. One of them is the filename under which the uploaded file has been temporarily stored. It is important to check that this variable was set by uploading a file. It might also be normal POSTed data, in which case you end up with this problem.

Securiteam: [NEWS] AeroMail Multiple Vulnerabilities

Problem #2

You can add additional headers to outgoing e-mail messages by sending some normal data for the To or CC or Subject fields, a CRLF and then another header with some data. (A lot of other programs allow this too. It's not just AeroMail.) This can be used for adding uuencoded attachments up in the headers with lines ending in CR instead of CRLF.

Problem #3

JavaScript and HTML code is active, when Subject headers are displayed. This allows DoS attacks by redirecting, theft of cookies etc.

Issues 1 and 2 require a valid user/password combination to be exploited, while issue 3 is open to anyone.

Solution:

The vendor was contacted with an explanation, two exploits and a patch on t