

# [NEWS] Active! mail Script Execution Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0057.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 06/15/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sat, 15 Jun 2002 21:44:31 +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.

-----

Active! mail Script Execution Vulnerability

---

## SUMMARY

Active! mail incorrectly displays messages without first filtering them for malicious content, this would allow an attacker to cause a user reading emails to unwittingly execute arbitrary code.

## DETAILS

Vulnerable systems:

- \* Active! mail version 1.422

- \* Active! mail version 2.0

Immune systems:

- \* Active! mail version 2.0.1.1

Active! mail developed and distributed by <A

href="http://www.transware.co.jp/">TransWARE</A> Co. is a web-based e-mail

system. Active! mail displays messages without filtering them properly for malicious code. If for example, a user receives an e-mail embedded with a malicious <script> tag in the header, the script will be executed upon the opening of the message.

Solution:

This problem can be eliminated by updating to Active! mail ver.2.0.1.1,

Securiteam: [NEWS] Active! mail Script Execution Vulnerability

which is available at:

<[http://www.transware.co.jp/active/download/am\\_download.html](http://www.transware.co.jp/active/download/am_download.html)>  
[http://www.transware.co.jp/active/download/am\\_download.html](http://www.transware.co.jp/active/download/am_download.html)

ADDITIONAL INFORMATION

The information has been provided by <mailto:[snsadv@lac.co.jp](mailto:snsadv@lac.co.jp)> Keigo Yamazaki (LAC).

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[NEWS] Cross-Site Scripting in Cisco Secure ACS"
  - *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)