

[UNIX] JAWmail XSS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0086.html>

From: support@securiteam.com

Date: 09/23/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 23 Sep 2002 16:07:50 +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.

JAWmail XSS

SUMMARY

Technically, <http://www.jawmail.org/> JAWmail's core is JAW -- a flexible framework for web application development; JAWmail it is packed with some applications and a simple, web based installer. Several cross-site scripting holes in JAWmail are triggered by reading incoming e-mail messages. An attacker can use them to take over a victim's e-mail account by simply sending certain malicious e-mails to the victim.

DETAILS

1) Read Mail shows the names of attached files without cleaning those names (removing HTML elements).

2) text/html mails are not cleaned at all, when they are shown in a pop-up window.

3) When Read Mail displays text/html mails, they are cleaned with PHP's `strip_tags()` function with some appropriate parameters. This function removes evil HTML elements, but not nice HTML elements with evil HTML attributes, so you can still perform XSS attacks like:

```
<b onmouseover="alert(document.cookie)">bolder</b>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:ulfh@update.uu.se> Ulf Harnhammar.

=====

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: "[NEWS] Flaws Found Within the Dynamic Host Configuration Protocol"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)