

[UNIX] kmMail Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0091.html>

From: support@securiteam.com

Date: 10/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: 21 Oct 2002 19:15:39 +0200

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.

kmMail Cross Site Scripting

SUMMARY

<<http://www.kmmail.org/>> kmMail is an open-sourced web-based mail client, based on Keftamail. A security vulnerability in the product allows remote attackers to insert malicious HTML and JavaScript into existing web pages making it appear as if the server was the one sending it.

DETAILS

Vulnerable systems:

- * kmMail version 1.0b and prior

Immune systems:

- * kmMail version 1.0b.1

kmMail has a cross-site scripting bug when viewing HTML e-mail messages. It filters out bad HTML elements, but not good HTML elements with bad HTML attributes like this one:

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

Solutions:

Users should upgrade to version 1.0b.1

Securiteam: [UNIX] kmMail Cross Site Scripting

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: "[TOOL] Simple EGG (Example)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)