

# [UNIX] Sympa Mailing List System Cross Site Scripting

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0074.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 08/22/04

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

Date: 22 Aug 2004 17:18:37 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Sympa Mailing List System Cross Site Scripting

---

## SUMMARY

<<http://www.sympa.org/>> Sympa is a rich open source mailing list software. Its design highly focuses on customization possibilities and ease of administration. The Sympa mailing list software is vulnerable to cross site scripting vulnerabilities.

## DETAILS

Vulnerable Systems:

- \* Sympa version 4.1.x

The creation list option is vulnerable to cross site-scripting attacks. It could allow an attacker to inject malicious HTML or script code into the system that can later be executed on a victim's machine. Normal uses for such attacks are cookie credential theft. Follow the steps below to test the vulnerability:

\* Navigate to <http://>/wvs>

\* Login with a valid e-mail and password (or click in the Send me Password option and follow the instructions)

Securiteam: [UNIX] Sympa Mailing List System Cross Site Scripting

- \* Click on create list option
- \* In the "List Name" field enter the text that you want
- \* In the "Subject" field enter the subject that you want
- \* Select your preferred topic
- \* In the description field insert the following text:  
<script>alert("Your cookie is " + document.cookie)</script>
- \* Click on "Submit your creation Request" button
- \* The list is created
- \* Now, click on "List Info". You will see your cookie in a JavaScript "alert" message box

Reference to the bug can be found in the Symba bug tracking list, at  
<[http://listes.cru.fr/mantis/view\\_bug\\_advanced\\_page.php?f\\_id=0000327](http://listes.cru.fr/mantis/view_bug_advanced_page.php?f_id=0000327)>  
[http://listes.cru.fr/mantis/view\\_bug\\_advanced\\_page.php?f\\_id=0000327](http://listes.cru.fr/mantis/view_bug_advanced_page.php?f_id=0000327).

ADDITIONAL INFORMATION

The information has been provided by <<mailto:joxeankoret@yahoo.es>> Joxean Koret.

=====

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.