

[UNIX] Mailman Multiple Security Issues

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00021.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 18 Sep 2006 18:52:37 +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>

Mailman Multiple Security Issues

SUMMARY

Mailman is "a mailing list server. It comes with a web based management interface, built-in archiving, automatic bounce processing, content filtering, digest delivery, spam filters, and more". Multiple security vulnerabilities have been discovered in Mailman product.

DETAILS

Vulnerable Systems:

- * Mailman versions 2.1.0 up to and including 2.1.8

Immune Systems:

- * Mailman version 2.1.9

Mailman is subject to multiple security vulnerabilities, ranging from cross site scripting to log file injection.

1. Cross Site Scripting (CVE-2006-3636)

Vulnerable versions of the application are subject to a XSS vulnerability in several functions and several parameters in the mailing list administration area of the web interface. An attacker may inject arbitrary

[UNIX] Mailman Multiple Security Issues

client side script code into several parameters through HTTP GET and POST method requests. Some of the injections will result in persistent injection of malicious scripting code.

To exploit these issues, prior successful authentication of the victim IS required. As such, only users who have a valid cookie for a specific mailing list stored in their client (including administrators who do not make use of the logout function) are vulnerable to this.

The following partial URLs demonstrate some of the issues:

```
[BaseURI]/mailman/admin/mailman/members?findmember=
%22%3E%3Cscript%3Ealert(0)%3B%3C/script%3E%3Cx%20y=%22
[BaseURI]/mailman/edithtml/tests/listinfo.html?html_code=
<h1>XSS%20demo</h1><scripT>alert(0)%3B</scripT>
```

2. Log file injection

The application is subject to a log injection vulnerability.

By injecting CRLF sequences followed by fake time stamps, an attacker may inject additional lines into the log files created by the application.

The following partial URL demonstrates this issue:

```
[BaseURI]/mailman/listinfo/doesntexist%22:%0D%0AJun
12%2018:22:08%202033%20mailmanctl(24851):
%22Your%20Mailman%20license%20has%20expired.%20Please%20obtain%20an%20upgrade%20at%20www.phishme.site%20
```

This will result in a message similar to the following to be written into /var/log/mailman/error.log:

```
Jun 11 18:50:43 2006 (32743) No such list "doesntexist":
jun 12 18:22:08 2033 mailmanctl(24851): "your mailman license
has expired. please obtain an upgrade at www.phishme.site"
```

Solutions:

The Mailman developers have released version 2.1.9 yesterday. This is supposed to fix all of the above issues. The updated packages are available at:

http://sf.net/project/showfiles.php?group_id=103&package_id=69562&release_id=447065
http://sf.net/project/showfiles.php?group_id=103&package_id=69562&release_id=447065

ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@xxxxxxxxxxxxxxxxxxxxxx>>
Moritz Naumann.

The original article can be found at:

<<http://moritz-naumann.com/adv/0013/mailmanmulti/0013.txt>>
<http://moritz-naumann.com/adv/0013/mailmanmulti/0013.txt>

[UNIX] Mailman Multiple Security Issues

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.