

# [UNIX] Majordomo Found to Leak Information

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-02/0005.html>

---

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

*Date:* 02/05/03

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

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

Date: 5 Feb 2003 01:43:19 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

Majordomo Found to Leak Information

---

## SUMMARY

A security vulnerability Majordomo, a PERL script for managing mailing lists, allows remote attackers and Spammers to query a mailing list for its complete address list.

## DETAILS

Vulnerable systems:

- \* Majordomo version 1.94.5 and prior
- \* Majordomo version 2

All email addresses can be extracted from mailing lists for which 'which\_access' is set to "open" in the configuration file, which\_access is set to "open" by default.

Majordomo 1.94.5 documentation quote:

"8. By default, anyone (even non-subscribers) can use the commands "who", "which", "index", and "get" on a list. If you create an empty file named "listname.private" in the \$listdir directory, only members of the list can use those commands."

## Securiteam: [UNIX] Majordomo Found to Leak Information

Typical case of RTFDOC of course, but still, why isn't the private configuration file the default one, now people actually have to read the documentation to protect their lists against evil spammers.

So this bug can be exploited without being subscribed to any mailing list on that server when "which\_access" is set to open. This bug can be exploited by sending:

```
which @
```

Or

```
which .
```

To the Majordomo daemon. Majordomo will then match "@" (or ".") on all the mailing lists that have 'which\_access' set to "open". This then matches all email addresses that are subscribed to that list.

There is a slight difference between the new Majordomo 2 (alpha) and the current Majordomo 1.94.x branch.

Majordomo 1.94.x gives output such as this:

```
>>>> which @
```

The string '@' appears in the following entries in lists served by [majordomo@somedomain.com](mailto:majordomo@somedomain.com):

List Address

```
==== =====
```

```
test-list user@somedomain.com
```

```
test-list anotheruser@anotherdomain.com
```

```
another-list satan@evilmajordomodomain.net
```

```
another-list bush@sopranos.org
```

etc...

Majordomo 2 also has the bug, not as much as the 1.94.x though:

```
>>>> which @
```

The pattern "\@/i" matched the following subscriptions.

Matches for the devils mailing list:

```
satan@majordomo.org
```

-- Match limit of 1 for devils exceeded.

Matches for the britney mailing list:

```
eminem@spears.net
```

-- Match limit of 1 for britney exceeded.

## Securiteam: [UNIX] Majordomo Found to Leak Information

### Impact:

High. Not only privacy is the issue here, this bug could be used by evil spammers to fill their databases. In addition, the users did much of their work for them already as the victims are usually well targeted (subject-specific mailing lists come to mind).

### Solution:

Read the documentation regarding \$listname.private and set all which\_access to "closed", or update to Majordomo 2 alpha, which still requires the same attention.

### Majordomo 1.94.5 and earlier:

As mentioned by the documentation that comes with Majordomo 1.94.5, create an empty file named "\$listname.private" in the \$listdir. It will only reduce the group of people being able to pick up all the addresses to the ones subscribed to the list. Check your current configurations for open which\_access and in case they are open, close them.

### Majordomo 2:

The authors responded quickly and changed default configuration settings to be "closed". Get the latest CVS version, and check your current configurations for open which\_access, which\_access should be closed at any time.

Jakub made a patch for Majordomo 1.94.5.

### Patch:

This is a patch for Majordomo 1.94.5, which makes the Majordomo ignore the 'which' request if they do not contain e-mail address-like string as a parameter (roughly).

```
--- majordomo.orig Mon Feb 3 13:23:45 2003
```

```
+++ majordomo Mon Feb 3 13:23:23 2003
```

```
@@ -624,6 +624,11 @@
```

```
sub do_which {
    local($subscriber) = join(" ", @_ ) || &valid_addr($reply_to);
+ if ($subscriber !~
+   /^[0-9a-zA-Z\.\-\_]+\@[0-9a-zA-Z\.\-\_]+\.[a-zA-Z]{2,3}$/) {
+
+   &log("which abuse -> $subscriber passed as an argument.");
+   exit(0);
+ };
    local($count, $per_list_hits) = 0;
    # Tell the requestor which lists they are on by reading through all
    # the lists, comparing their address to each address from each list
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[m.v.berkum@obit.nl](mailto:m.v.berkum@obit.nl)> Marco van Berkum and <mailto:[jacke@bofh.pl](mailto:jacke@bofh.pl)> Jakub Klausa.

Securiteam: [UNIX] Majordomo Found to Leak Information

=====

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.