

# [UNIX] Mandrake MSec Security Issue

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0112.html>

---

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

*Date:* 06/23/02

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

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

Date: Sun, 23 Jun 2002 21:37:39 +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.

-----

Mandrake MSec Security Issue

---

## SUMMARY

MSec utility provides a simple and efficient way to tune the security of a system accordingly to its intended purpose. A security vulnerability in the default security settings leave users' home directories world readable.

## DETAILS

Vulnerable systems:

- \* Mandrake version 8.2

Immune systems:

- \* Mandrake version 8.1

The Mandrake Security a.k.a MSec level (as offered as the default choice during the install) is set at "Standard", described as in the Mandrake Control Center as "the standard security recommended for a computer that will be used to connect to the Internet as a client", has been found to leave the home directories of user with world readable settings.

Vendor contact:

Multiple email and forms contacts have been tried, as of this date, no response from Mandrake.

Securiteam: [UNIX] Mandrake MSec Security Issue

Solutions/Workarounds:

Until this is acknowledged/handled by Mandrake, administrators should use the Mandrake Control Center, security settings section, and make sure the level is set to at least "High", or manually enter 'msec 3' via CLI, not the default, "Standard" a.k.a 'msec 2', security level. The msec package can also be removed entirely (after the system is installed) and permissions set manually after that.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[spot@getlinuxonline.com](mailto:spot@getlinuxonline.com)>  
Spot.

=====

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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] DPGS Allows Any File to Be Overwritten"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)