

[NT] MondoSearch Show Source of Arbitrary Files

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0094.html>

From: support@securiteam.com

Date: 10/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: 21 Oct 2002 20:13:50 +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.

MondoSearch Show Source of Arbitrary Files

SUMMARY

<<http://www.mondosoft.com/>> MondoSearch is an enterprise-class search engine for Internet sites, Intranets, Extranets or Portals environments.

Due to a vulnerability in the product a remote attacker can see the source of the files.

DETAILS

Vulnerable systems:

- * MondoSearch version 4.4

Example:

To see the source of the file foo.asp setting in the root directory request the following URL:

<http://foo/cgi-bin2/MsmMask.exe?mask=/foo.asp>

Vendor status:

Although the MondoSoft was not notified prior to the posting, MondoSoft has reacted quickly and have remedied the situation within 24 hours by which time all MondoSoft customers where notified. See the following:

Secure your site without updating:

<<http://www.mondosoft.com/security-info.asp>>

<http://www.mondosoft.com/security-info.asp>

Securiteam: [NT] MondoSearch Show Source of Arbitrary Files

Obtaining an update: <<http://www.mondosoft.com/security-update.asp>>
<http://www.mondosoft.com/security-update.asp>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:thefastkid@ziplip.com>>
thefastkid and <<mailto:orp644@yahoo.com>> Orp 664.

=====

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: "[NEWS] Full Zone Information Disclosure on Top Level Domain Name Servers"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)