

# [NEWS] Lotus iNotes Client ActiveX Control Buffer Overrun

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-02/0039.html>

---

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

*Date:* 02/17/03

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

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

Date: 17 Feb 2003 22:26:18 +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)

-----

Lotus iNotes Client ActiveX Control Buffer Overrun

---

## SUMMARY

Lotus Domino and Notes together provide a featured enterprise collaboration system with Domino providing application server services. iNotes provides web based messaging facilities. As well as having a server component there exists a client ActiveX control. A vulnerability in the ActiveX client allows a remote attacker to cause it to overflow one of its internal buffers allowing him to effectively compromise the remote host.

## DETAILS

Vulnerable systems:

- \* Lotus Domino version 6.0

Immune systems:

- \* Lotus Domino version 6.0.1

When iNotes is installed there is an ActiveX control called Lotus Domino Session ActiveX Control. By supplying an overly long value to the "InitializeUsingNotesUserName" method of this control via an e-mail or web page it is possible for an attacker to execute arbitrary code on the target's local machine. Any exploit code would execute in the security

Securiteam: [NEWS] Lotus iNotes Client ActiveX Control Buffer Overrun

context of the logged on user.

Fix Information:

NGSSoftware alerted IBM/Lotus to this issue on 14 January 2002. IBM Lotus Notes and Domino Release 6.0.1 is now available and being marketed as the first maintenance release. IBM say if customers haven't already upgraded or migrated to Notes and Domino 6, now is the time to move and start reaping the benefits of this existing and highly praised release. Release 6.0.1 includes fixes to enhance the quality and reliability of the Notes and Domino 6 products. It does not however mention any security issues, and NGS would strongly advise to upgrade as soon as possible not to just to "reap the benefits" but to secure the server and data against possible attacks.

The upgrade / patch can be obtained from

<<http://www14.software.ibm.com/webapp/download/search.jsp?q=&cat=&pf=&k=&dt=&go=y&rs=ESD-NOTECLN>>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@nextgenss.com>>  
NGSSoftware Insight Security Research.

=====

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.