

[NEWS] Lotus Domino Web Server iNotes Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-02/0041.html>

From: support@securiteam.com

Date: 02/17/03

From: support@securiteam.com

To: list@securiteam.com

Date: 17 Feb 2003 22:21:43 +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

Lotus Domino Web Server iNotes Overflow

SUMMARY

Lotus Domino and Notes together provide a featured enterprise collaboration system with Domino providing application server services. iNotes provides web based messaging facilities. A remotely exploitable buffer overflow allows an attacker to overflow an internal buffer used by the Lotus Domino server allowing him to compromise the server (by causing it to execute arbitrary code).

DETAILS

Vulnerable systems:

- * Lotus Domino version 6.0

Immune systems:

- * Lotus Domino version 6.0.1

iNotes suffers from a remotely exploitable buffer overrun when an attacker provides an overly long value for the s_ViewName/Foldername options of the PresetFields parameter when requesting web based mail services. Any code supplied would run in the security context of the account running the Domino Web Services.

Securiteam: [NEWS] Lotus Domino Web Server iNotes Overflow

Fix Information:

NGSSoftware alerted IBM/Lotus to this issue on the 14 of 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-DMNTRV>>

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
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.