	Authorisation. Jason Edelstein
	Release date. 9 July 2009.

Sense of Security – Security Advisory – SOS-09-004.

Lotus Sametime User Enumeration Vulnerability.

9 July 2009.

Lotus Sametime User Enumeration Vulnerability - Security Advisory – SOS-09-004

Release Date.	9-Jul-2009
Last Update.	-
Vendor Notification Date.	2-Jun-2009
Product.	IBM Lotus Instant Messaging and Web Conferencing (Sametime)
Platform.	Windows (verified), possibly others
Affected versions.	IBM Lotus Instant Messaging and Web Conferencing (Sametime) 6.5.1 (verified), possibly others
Severity Rating.	Low
Impact.	Exposure of sensitive information
Attack Vector.	Remote without authentication
Solution Status.	Vendor patch not yet available
CVE reference.	Not yet allocated

Details.

IBM Lotus Sametime is an enterprise instant messaging and web conferencing application. During an application penetration test Sense of Security identified a user enumeration vulnerability when trying to connect to the Sametime server using the Sametime Connect Client. This occurred as a result of varying response times depending on whether or not a valid user name is supplied.

The client takes significantly longer to display the 'Invalid logon' error message when a valid username (and invalid password) is provided (5-8 seconds). This is a result of additional information exchanges occurring between the server and client.

When an invalid username (and password) is supplied, the error is displayed almost instantaneously (1-3 seconds).

This can be used to enumerate valid user names.

Solution.

The vendor has advised that IBM is looking to eliminate this behaviour completely in a future release.

Discovered by.

Karan Khosla from SOS Labs.

About us.

Sense of Security is a leading provider of IT security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application security consultancy and trusted IT security advisor to many of the countries largest organisations.

Sense of Security Pty Ltd

Level 3, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-09-004.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php