

Advisory: SQL Injection Vulnerability in the MSN Messenger Forums

Vendor :
MSN [MSN Messenger Forums]

Severity : Critical

Dated : 31 October 2006

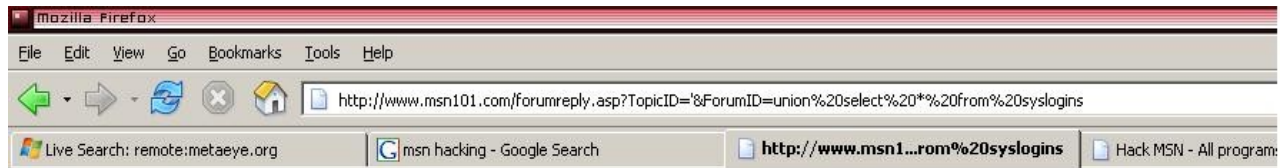
By: Aditya K Sood [www.secniche.org]

Explanation:

A severe SQL injection vulnerability occurred in the MSN messenger forums website. This injection reveals the database name with other table specification. The vulnerability is the result of false input which can not be handled by the server there by disclosing the information.

Website : <http://www.msn101.com/forumreply.asp?TopicID=320&ForumID=2>

Output :



Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value 'union select * from syslogins' to a column of data type int.

/includes/configdb.asp, line 48

Vendor Status : Reported and Patched