

Alert: Microsoft Security Bulletin – MS03–026

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-07/0042.html>

From: Russ (*Russ.Cooper_at_RC.ON.CA*)

Date: 07/16/03

Date: Wed, 16 Jul 2003 13:01:19 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

<http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>

Buffer Overrun In RPC Interface Could Allow Code Execution (823980)

Originally posted: July 16, 2003

Summary

Who should read this bulletin: Users running Microsoft ® Windows ®

Impact of vulnerability: Run code of attacker's choice

Maximum Severity Rating: Critical

Recommendation: Systems administrators should apply the patch immediately

End User Bulletin: An end user version of this bulletin is available at:

http://www.microsoft.com/security/security_bulletins/ms03-026.asp.

Affected Software:

- Microsoft Windows NT® 4.0
- Microsoft Windows NT 4.0 Terminal Services Edition
- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server(tm) 2003 Not Affected Software:
- Microsoft Windows Millennium Edition

Technical description:

Remote Procedure Call (RPC) is a protocol used by the Windows operating system. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. The protocol itself is derived from the Open Software Foundation (OSF) RPC protocol, but with the addition of some Microsoft specific extensions.

There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a Distributed

