

# Microsoft RPC Locator Buffer Overflow Vulnerability (#NISR29012003)

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-01/0051.html>

---

**From:** NGSSoftware Insight Security Research ([nisr@NEXTGENSS.COM](mailto:nisr@NEXTGENSS.COM))

**Date:** 01/30/03

Date: Thu, 30 Jan 2003 04:27:51 -0000  
From: NGSSoftware Insight Security Research <[nisr@NEXTGENSS.COM](mailto:nisr@NEXTGENSS.COM)>  
To: [NTBUGTRAO@LISTSERV.NTBUGTRAO.COM](mailto:NTBUGTRAO@LISTSERV.NTBUGTRAO.COM)

NGSSoftware Insight Security Research Advisory

Name: Locator Service Buffer Overflow Vulnerability

Systems Affected: Windows 2000/XP/NT

Severity: High Risk / Critical

Category: Buffer Overrun

Vendor URL: <http://www.microsoft.com/>

Author: David Litchfield ([david@ngssoftware.com](mailto:david@ngssoftware.com))

Date: 29th January 2003

Advisory number: #NISR29012003

Tool: <http://www.ngssoftware.com/rpclocator.html>

## Description

\*\*\*\*\*

There is a remotely exploitable buffer overflow vulnerability in the Microsoft RPC (Remote Procedure Call) Locator Service on Windows platforms. The RPC Locator Service maintains a list of RPC services and servers on the network. Typically only domain controllers run the Locator service by default and these machines are the most at risk.

## Details

\*\*\*\*\*

When searching for RPC Services on the network a Windows RPC client will connect to the domain controller over TCP port 139/445 (the SMB ports) and search for services/servers through the "locator" named pipe. An attacker can overflow a stack based buffer in the Locator service process by searching for an overly long string for an entry name to use in looking for binding handles. This problem arises due to an unsafe call to `wscpy()`.

## Fix Information

\*\*\*\*\*

NGSSoftware advised Microsoft to this problem at the end of October of 2002. Microsoft released the patch to resolve this issue last week.

[http://www.microsoft.com/security/security\\_bulletins/ms03-001.asp](http://www.microsoft.com/security/security_bulletins/ms03-001.asp)



NT-Bugtraq: Microsoft RPC Locator Buffer Overflow Vulnerability (#NISR29012003)

oo