

# Alert: Microsoft Security Bulletin MS04-020 – Vulnerability in POSIX Could Allow Code Execution (841872)

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-07/0023.html>

---

**From:** Russ (*Russ.Cooper\_at\_RC.ON.CA*)

**Date:** 07/13/04

Date: Tue, 13 Jul 2004 14:22:16 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Microsoft Security Bulletin MS04-020:  
Vulnerability in POSIX Could Allow Code Execution (841872)

Bulletin URL:

<<http://www.microsoft.com/technet/security/bulletin/MS04-020.msp>>

Version Number: 1.0

Issued Date: Tuesday, July 13, 2004

Impact of Vulnerability: Local Elevation of Privilege

Maximum Severity Rating: Important

Patch(es) Replaced: None

Caveats: None

Tested Software:

Affected Software:

-----  
\* Microsoft Windows NT. Workstation 4.0 Service Pack 6a

<<http://tinyurl.com/4dpou>>

\* Microsoft Windows NT Server 4.0 Service Pack 6a

<<http://tinyurl.com/59vkv>>

\* Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

<<http://tinyurl.com/72adx>>

\* Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000 Service Pack 3, Microsoft Windows 2000 Service Pack 4

<<http://tinyurl.com/3hph2>>

Technical Description:

-----  
\* POSIX Vulnerability – CAN-2004-0210 A privilege elevation vulnerability exists in the POSIX subsystem. This vulnerability could allow a logged on user to take complete control of the system.

This email is sent to NTBugtraq automatically as a service to my subscribers. (v4.01.1642.17968)

Alert: Microsoft Security Bulletin MS04-020 – Vulnerability in POSIX Could Allow Code Execution (841872)

NT-Bugtraq: Alert: Microsoft Security Bulletin MS04-020 – Vulnerability in POSIX Could Allow Code Execution (841872)

Cheers,

Russ – Senior Scientist – TruSecure Corporation/NTBugtraq Editor

-----

NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting reply is going to result in the message coming to the list, not to the individual who sent the message. This was done to help reduce the number of Out of Office messages posters received. So if you want to send a reply just to the poster, you'll have to copy their email address out of the message and place it in your TO: field.

-----

Alert: Microsoft Security Bulletin MS04-020 – Vulnerability in POSIX Could Allow Code Execution (841872)