

# Microsoft Security Bulletin MS02-024

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2002-05/0554.html>

---

**From:** Jerry Bryant [MS] ([jbryant@online.microsoft.com](mailto:jbryant@online.microsoft.com))

**Date:** 05/23/02

From: "Jerry Bryant [MS]" <[jbryant@online.microsoft.com](mailto:jbryant@online.microsoft.com)>

Date: Wed, 22 May 2002 16:05:56 -0700

**Title:** Authentication Flaw in Windows Debugger can Lead to  
Elevated Privileges (Q320206)

**Date:** 22 May 2002

**Software:** Microsoft Windows

**Impact:** Elevation of Privilege

**Max Risk:** Critical

**Bulletin:** MS02-024

Microsoft encourages customers to review the Security Bulletin at:  
<http://www.microsoft.com/technet/security/bulletin/MS02-024.asp>.

---

**Issue:**

=====

The Windows debugging facility provides a means for programs to perform diagnostic and analytic functions on applications as they are running on the operating system. One of these capabilities allows for a program, usually a debugger, to connect to any running program, and to take control of it. The program can then issue commands to the controlled program, including the ability to start other programs. These commands would then execute in the same security context as the controlled program.

There is a flaw in the authentication mechanism for the debugging facility such that an unauthorized program can gain access to the debugger. A vulnerability results because an attacker can use this to cause a running program to run a program of her choice. Because many programs run as the operating system, this means that an attacker can exploit this vulnerability to run code as the operating system itself. She could take any action on the system including deleting data, adding accounts with administrative access, or reconfiguring the system.

A successful attack requires the ability to logon interactively to the system, either at the console or through a terminal session. Also, an a successful attack requires the introduction of code to exploit this vulnerability. Because best practices recommends restricting the ability to

logon interactively on servers, this issue most directly affects client systems and terminal servers.

Mitigating Factors:

=====

- A successful attack requires the ability to logon interactively to the target machine, either directly at the console or through a terminal session. Best practices strongly militate against ever allowing an unprivileged user to interactively log onto business-critical systems such as ERP servers, database servers, domain controllers and the like. If these recommendations have been followed, the vulnerability would principally pose a threat only to systems like workstations and terminal servers.
- A successful attack requires that the attacker be able to load code of her choice on the system. Restrictions on a user's ability to load and execute arbitrary code could potentially prevent a successful attack.

Risk Rating:

=====

- Internet systems: Low
- Intranet systems: Moderate
- Client systems: Critical

Patch Availability:

=====

- A patch is available to fix this vulnerability. Please read the Security Bulletin at <http://www.microsoft.com/technet/security/bulletin/ms02-024.asp> for information on obtaining this patch.

-----

THE INFORMATION PROVIDED IN THE MICROSOFT KNOWLEDGE BASE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MICROSOFT CORPORATION OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF MICROSOFT CORPORATION OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

--

Regards,  
Jerry Bryant - MCSE, MCDBA  
Microsoft IT Communities

microsoft.public.security: Microsoft Security Bulletin MS02-024

Get Secure! [www.microsoft.com/security](http://www.microsoft.com/security)

This posting is provided "AS IS" with no warranties, and confers no rights.