

Revised: Microsoft Security Bulletin – MS02–017

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-04/0062.html>

From: Russ (Russ.Cooper@RC.ON.CA)

Date: 04/16/02

Date: Tue, 16 Apr 2002 13:10:35 -0400

From: Russ <Russ.Cooper@RC.ON.CA>

To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

This bulletin has been revised.

V1.0 (April 04, 2002): Bulletin Created.

V1.1 (April 16, 2002): Bulletin updated to clarify that Windows XP Home Edition is also affected.

Original bulletin details follow;

<http://www.microsoft.com/technet/security/bulletin/MS02-017.asp>

Unchecked buffer in the Multiple UNC Provider Could Enable Code Execution (Q311967)

Originally posted: April 04, 2002

Summary

Who should read this bulletin: Customers using Microsoft® Windows NT®, Windows® 2000 and Windows XP

Impact of vulnerability: Local privilege elevation and run code of attacker's choice.

Maximum Severity Rating: Moderate

Recommendation: Administrators should consider applying the patch to machines that allow unprivileged users to log onto them interactively such as workstations and Terminal Servers.

Affected Software:

- Microsoft Windows NT 4.0 Workstation
- Microsoft Windows NT 4.0 Server
- Microsoft Windows NT 4.0 Server, Enterprise Edition
- Microsoft Windows NT 4 Terminal Server Edition
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows XP Home
- Microsoft Windows XP Professional

Technical description:

NT-Bugtraq: Revised: Microsoft Security Bulletin – MS02–017

The Multiple UNC Provider (MUP) is a Windows service that assists in locating network resources that are identified via UNC (uniform naming convention). The MUP receives commands containing UNC names from applications and sends the name to each registered UNC provider, LAN Manager workstation, and any others that are installed. When a provider identifies a UNC name as its own, the MUP automatically redirects future instances of that name to that provider.

When MUP receives a file request, it allocates a buffer in which to store it. There is proper input checking in this first buffer. However, MUP stores another copy of the file request in a buffer when it sends this request to a redirector. This second copy of the buffer does not check inputs correctly, thereby creating the possibility that a resource request to it from an unprivileged process could cause a buffer overrun. The overrun could be exploited for either of two purposes: causing a system failure, or running code on the system with Local System privileges.

Mitigating factors:

- The MUP request can only be levied by a process on the local system. As a result, the vulnerability could only be exploited by a user who could log onto an affected system interactively.
- On Windows 2000 systems, the vulnerability could not reliably be used to run code. This is because the attacker would need to know where the buffer was located in memory, but in Windows 2000 this is not externally discoverable or controllable. .
- Best practices suggests that unprivileged users not be allow to interactively log onto business–critical servers. If this recommendation has been followed machines such as domain controllers, ERP servers, print and file servers, database servers, and others would not be at risk from this vulnerability.

Vulnerability identifier: CAN–2002–0151

This email is sent to NTBugtraq automatically as a service to my subscribers. Since its programmatically created, and since its been a long time since anyone paid actual money for my programming skills, it may or may not look that good...;-]

I can only hope that the information it does contain can be read well enough to serve its purpose.

Cheers,

Russ – Surgeon General of TruSecure Corporation/NTBugtraq Editor

- *Previous message:* [Arne Vidstrom: "Announcing PromiscDetect"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)