

# Microsoft Utility Manager Local Privilege Escalation

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-07/0031.html>

---

**From:** NGSSoftware Insight Security Research (*nistr\_at\_NEXTGENSS.COM*)

**Date:** 07/09/03

Date: Wed, 9 Jul 2003 18:35:08 +0100

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

NGSSoftware Insight Security Research Advisory

Name: Microsoft Utility Manager Local Privilege Escalation

Systems Affected: Windows 2000 SP3

Severity: Medium Risk

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

Authors: Chris Paget [ [foon@ngssoftware.com](mailto:foon@ngssoftware.com) ]

Chris Anley [ [chris@ngssoftware.com](mailto:chris@ngssoftware.com) ]

Sherief Hammad [ [sherief@ngssoftware.com](mailto:sherief@ngssoftware.com) ]

Date Vendor Notified: 30th April 2003

Date of Public Advisory: 9th July 2003

Advisory number: #NISR09072003

Advisory URL: <http://www.ngssoftware.com/advisories/utilitymanager.txt>

## Description

\*\*\*\*\*

Microsoft Windows 2000 provides extensive "accessibility" features, that allow disabled users to more easily make use of the operating system.

Tools such as the Windows Narrator (that translates on-screen text into audible speech) and the On Screen Keyboard (that allows a user to simulate a keyboard using only a pointing device) are an integral part of the operating system and can be started at any time via the Windows 'Utility Manager'.

In Windows 2000, the utility manager runs in the context of the local 'system' account and can be started in the desktop of any user.

The Utility Manager is vulnerable to a 'Shatter' style privilege escalation involving the "ListView" control in its main window.

## Details

\*\*\*\*\*

## NT-Bugtraq: Microsoft Utility Manager Local Privilege Escalation

By pressing the '<windows key>+U' key combination at any time, a user can start the Windows Utility Manager. The utility manager process is (indirectly) started by the Winlogon process, and runs in the context of the 'system' account, in the desktop of the user that invoked it.

Interestingly, the utility manager can also be started directly at the login prompt, by pressing <windows key>+U.

The main Utility Manager window contains a ListView control that details the available accessibility tools. Windows messages sent directly to this control are not validated and it is thus possible to perform a number of dangerous interactions with the Utility Manager process.

A couple of interesting messages in this context are the LVM\_SORTITEMS and LVM\_SORTITEMSEX messages, that instruct the list box control to 'sort' its contents based using a callback function whose address is specified in the message.

By modifying window text and then sending an LVM\_SORTITEMS message to the list control, it is possible to make the Utility Manager process jump to code supplied by the (low-privileged) user. This code is then executed in the context of the local 'system' account.

The exploit code needed is functionally equivalent to previous 'shatter' code, with the only substantial difference being the use of the 'LVM\_SORTITEMS' message rather than the 'WM\_TIMER' message.

### Fix Information

\*\*\*\*\*

Microsoft have supplied a patch for this problem that can be downloaded from:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-025.asp>

This patch is included in Windows 2000 Service Pack 4.

### Further Information

\*\*\*\*\*

Chris Paget will be speaking about this bug and other Shatter – related matters at the Blackhat Briefings. For more information, see

<http://www.blackhat.com/html/bh-usa-03/bh-usa-03-speakers.html#Chris%20Paget>

### About NGSSoftware

\*\*\*\*\*

NGSSoftware design, research and develop intelligent, advanced application security assessment scanners. Based in the United Kingdom, NGSSoftware have offices in the South of London and the East Coast of Scotland. NGSSoftware's sister company NGSConsulting, offers best of breed security

