

[NT] Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0052.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/14/03

To: list@securiteam.com

Date: 14 Jul 2003 17:11:41 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation

SUMMARY

Microsoft Windows 2000 contains support for Accessibility options within the operating system. Accessibility support is a series of assistive technologies within Windows that allow users with disabilities to still be able to access the functions of the operating system. Accessibility support is enabled or disabled through shortcuts built into the operating system, or through the Accessibility Utility Manager. Utility Manager is an accessibility utility that allows users to check the status of accessibility programs (Microsoft Magnifier, Narrator, On-Screen Keyboard) and to start or stop them.

There is a flaw in the way that Utility Manager handles Windows messages. Windows messages provide a way for interactive processes to react to user events (for example, keystrokes, or mouse movements) and communicate with other interactive processes. A security vulnerability results because the control that provides the list of accessibility options to the user does

Securiteam: [NT] Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation

not properly validate Windows messages sent to it. It's possible for one process in the interactive desktop to use a specific Windows message to cause the Utility Manager process to execute a callback function at the address of its choice. Because the Utility Manager process runs at higher privileges than the first process, this would provide the first process with a way of exercising those higher privileges. By default, the Utility Manager contains controls that run in the interactive desktop with Local System privileges. As a result, an attacker who had the ability to log on to a system interactively could potentially run a program that could send a specially crafted Windows message upon the Utility Manager process, causing it to take any action the attacker specified. This would give the attacker complete control over the system.

The attack cannot be exploited remotely, and the attacker would have to have the ability to interactively log on to the system.

DETAILS

Vulnerable systems:

- * Microsoft Windows 2000

Immune systems:

- * Microsoft Windows Me
- * Microsoft Windows NT Server 4.0
- * Microsoft Windows NT Server, Terminal Services Edition
- * Microsoft Windows XP
- * Microsoft Windows Server 2003

Mitigating factors:

* An attacker would need valid logon credentials to exploit the vulnerability. It could not be exploited remotely.

* Properly secured servers would be at little risk from this vulnerability. Standard best practices recommend only allowing trusted administrators to log on to such systems interactively; without such privileges, an attacker could not exploit the vulnerability.

What's the scope of the vulnerability?

This is a

<http://www.microsoft.com/technet/security/bulletin/glossary.asp> privilege elevation vulnerability. An attacker who successfully exploited this vulnerability could gain unwarranted privileges on a system. In this case, the attacker could gain full administrative privileges, thereby gaining the ability to take any action they want on the machine, such as adding, deleting, or modifying data on the system, creating or deleting user accounts, and adding accounts to the local administrators group. An attacker who had credentials to log on to the computer interactively could only exploit the vulnerability. Best practices suggest that unprivileged users not be allowed to interactively log on to business-critical servers; if this guidance has been followed, such servers would not be at risk from this vulnerability. Instead, the systems primarily at risk would be

workstations and terminal servers.

What causes the vulnerability?

The vulnerability results because it is possible for an unprivileged user to cause code to be executed by a highly privileged process on the interactive desktop using Utility Manager in combination with a specially crafted Windows message.

Microsoft recognizes its responsibility to develop technology that is accessible and usable to everyone, including those with disabilities.

Therefore, all Microsoft products are designed with functionality and utilities to assist in enabling those with disabilities to use the features of the products. These utilities are known as Accessibility utilities. Windows 2000 contains several utilities and technologies to provide accessibility within the product. A detailed list of these utilities can be found at:

<<http://www.microsoft.com/enable/products/windows2000/features.aspx>>
<http://www.microsoft.com/enable/products/windows2000/features.aspx>

Where does Microsoft document the available Accessibility options in its products?

More information on accessibility options within Microsoft Products can be found at the Microsoft Accessibility Web site at:

<<http://www.microsoft.com/enable/>> <http://www.microsoft.com/enable/>

What is the Utility Manager?

Utility Manager is an accessibility utility that allows users to check the status of accessibility programs (Microsoft Magnifier, Narrator, On-Screen Keyboard) and to start or stop them.

What do you mean by a "desktop"?

Normally, when we refer to a "desktop" we mean the Windows desktop created by Explorer that you see on your screen during a Windows session. However, in the Windows security architecture, the term "desktop" actually has a different meaning. Desktops are used to encapsulate windows and related objects in Windows in order to ensure that a process is properly restricted to only activities that are authorized. It is easier to explain what a desktop is and how it works if we start with the layer of granularity above the desktop, the windows station.

What is a windowstation?

A windowstation is a container that contains a clipboard, some global information, and a set of one or more desktops. The interactive windowstation assigned to the logon session of the interactive user also contains the keyboard, mouse, and display device. The interactive windowstation is visible to the user and can receive input from the user. All other windowstations are non-interactive, which means that they cannot be made visible to the user and cannot receive user input. A process can be associated with only one desktop at a time.

Securiteam: [NT] Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation

What's an interactive desktop?

A desktop is a container object that is contained within a window station. There may be many desktops contained within a windowstation.

A desktop has a logical display surface and contains windows, menus, and hooks. Only the desktops of the interactive window station can be visible and receive user input. On the interactive windowstation, only one desktop at a time is active. This active desktop, also referred to as the interactive desktop or input desktop, is the one that is currently visible to the user and that receives user input.

What are Windows messages?

Processes running on Windows interact with the system and other processes using

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winui/WinUI/WindowsUserInterface/Windowing/M>

essages. For instance, each time the user hits a key on the keyboard, moves the mouse, or clicks a control such as a scroll bar, Windows generates a message, the purpose of which is to alert the program that a user event has occurred, and deliver the data from that event to the program. Similarly, a program can generate messages as a way of allowing the various windows it controls to communicate with and task each other.

What's wrong with the way Windows messages are handled by the Windows 2000 Utility Manager?

The flaw actually lies in the way Utility Manager handles messages when presenting the list of available accessibility functions to the user.

Utility Manager does not properly validate Windows messages sent to it. If Utility Manager is running on the system, it is possible for another process running on the system to send a specially crafted message to the Utility Manager process in the interactive desktop. The first process could set the address of the callback function, with the result being that the second process would execute the callback function specified by the first.

Why does this pose a security vulnerability?

Essentially, the flaw in Utility Manager would provide a way for one process on the interactive desktop to cause the Utility Manager to do its bidding. If the second process had higher privileges, this would provide a way for the first to exercise them.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited the vulnerability could first start Utility Manager, then could create a process that would levy requests upon the Utility Manager once it was running. In default configurations of Windows 2000, Utility Manager is installed but not running. Exploiting the vulnerability in such a case would enable the attacker to gain complete control over the system.

Who could exploit the vulnerability?

To exploit the vulnerability, the attacker would need the ability to log on to the system, start Utility Manager, load a program of his or her choice (one that sent a message to Utility Manager and specified a callback function that would perform some desired task), and run it.

Securiteam: [NT] Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation

What versions of the Utility Manager are vulnerable to this attack?

Only the Windows 2000 version of Utility Manager contains the vulnerability. Windows NT Server 4.0, Windows XP, and Windows Server 2003 are not affected.

What systems are primarily at risk from the vulnerability?

In general, workstations and terminal servers would be mainly at risk. Servers would only be at risk if unprivileged users had been given the ability to log on to them and run programs, but best practices strongly discourage allowing this. Could the vulnerability be exploited from the Internet? No. The attacker would need the ability to log on to the specific system he or she wished to attack. There is no capability to load and run a program in the interactive desktop remotely. What does the patch do? The patch addresses the vulnerability by changing the handling of Windows messages by the Utility Manager so that messages are properly validated and that an unregistered callback function cannot be called.

Patch availability

<http://microsoft.com/downloads/details.aspx?FamilyId=D415A4AC-E13A-4E8A-BE25-85E7DF686F61&displayl>
<http://microsoft.com/downloads/details.aspx?FamilyId=D415A4AC-E13A-4E8A-BE25-85E7DF686F61&displayl>

ADDITIONAL INFORMATION

The vulnerability was discovered by: Chris Paget of
<http://www.nextgenss.com> Next Generation Security Software Ltd.

The original article can be found at:
<http://www.microsoft.com/technet/security/bulletin/MS03-025.asp>

The information has been provided by Microsoft Product Security.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.