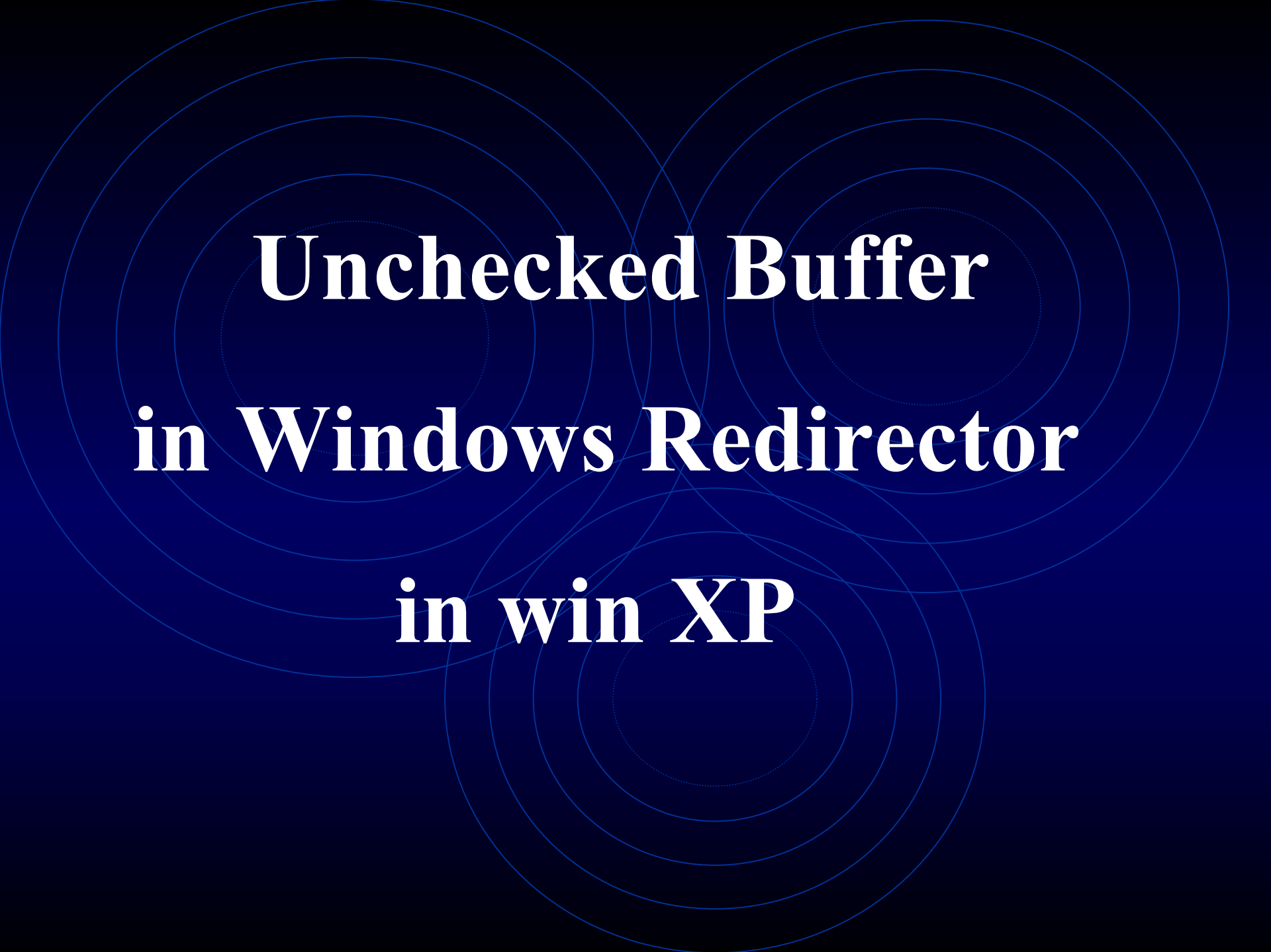


Attack windows vulnerability

- By Lu Xiaojun



Unchecked Buffer
in Windows Redirector
in win XP

A security vulnerability exists in the Windows Redirector of Windows XP that could allow a local user to elevate their security privileges by exploiting an unchecked buffer.

Issue

The Windows Redirector is used by a Windows client to access files, whether local or remote, regardless of the underlying network protocols in use. For example, the "Add a Network Place" Wizard or the NET USE command can be used to map a network share as a local drive, and the Windows Redirector will handle the routing of information to and from the network share.

A security vulnerability exists in the implementation of the Windows Redirector on Windows XP because an unchecked buffer is used to receive parameter information. By providing malformed data to the Windows Redirector, an attacker could cause the system to fail, or if the data was crafted in a particular way, could run code of the attacker's choice.

The background is a dark blue gradient with several overlapping, concentric circles of a lighter blue color. The text is centered in the upper half of the image.

Unchecked Buffer in Windows Shell

An unchecked buffer exists in one of the functions used by the Windows Shell to extract custom attribute information from audio files. This could allow a malicious user to mount a buffer overrun attack and possibly run the code of their choice on the system.

Issue

The Windows Shell is responsible for providing the basic framework of the Windows user interface experience. It is most familiar to users as the Windows Desktop, but also provides a variety of other functions to help define the user's computing session, including organizing files and folders, and providing the means to start applications.



Affected operating system

Microsoft Windows XP



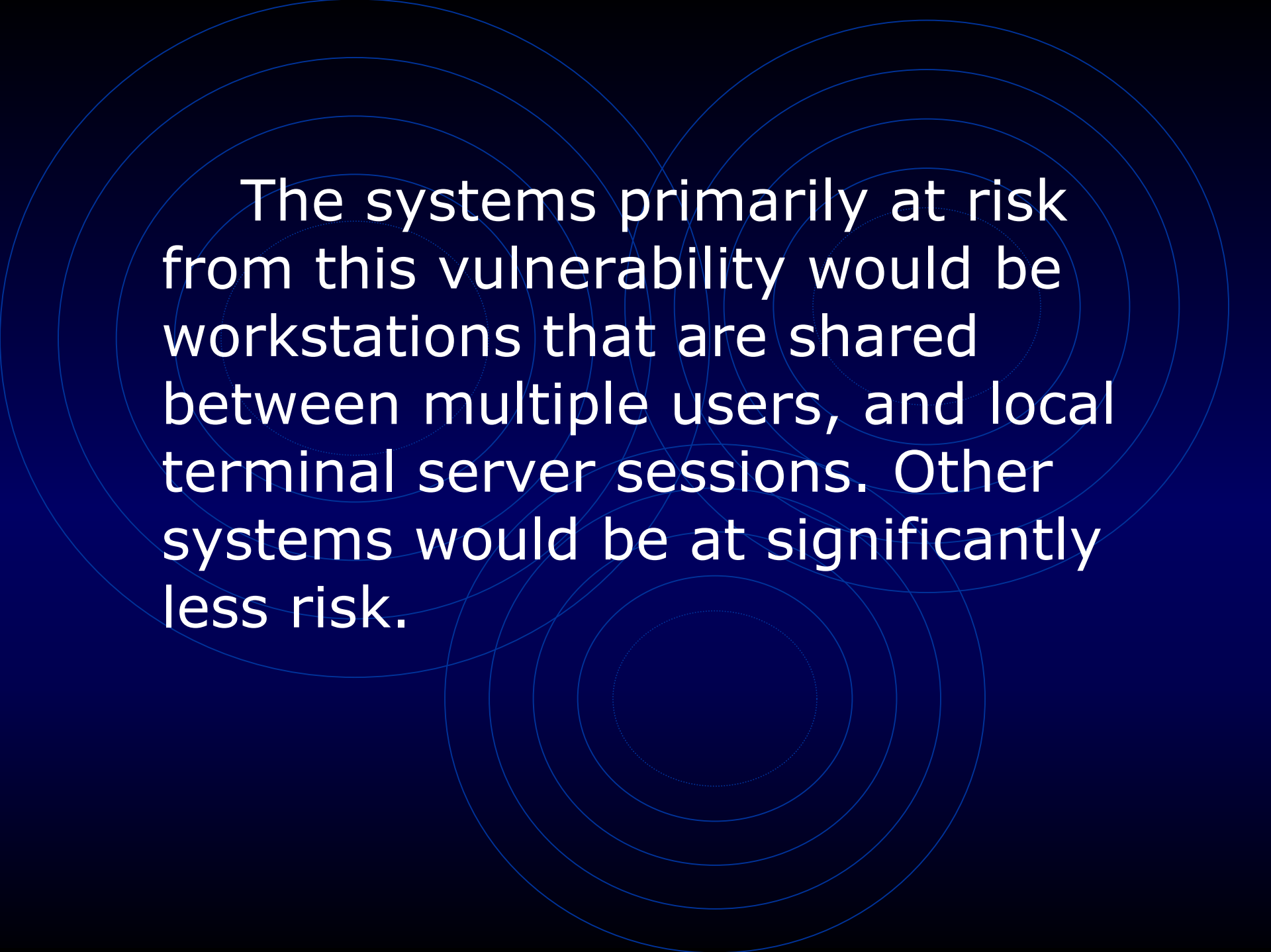
**Windows2000
Default Permissions
Could Allow Trojan
Horse Program**

Due to the default permissions used on the Windows 2000 system root folder it could enable an attacker to mount a Trojan horse attack against other users of the same system.

Issue

On Windows 2000, the default permissions provide the Everyone group with Full access (Everyone:F) on the system root folder (typically, C:\). In most cases, the system root is not in the search path. However, under certain conditions – for instance, during logon or when applications are invoked directly from the Windows desktop via Start | Run – it can be.

This situation gives rise to a scenario that could enable an attacker to mount a Trojan horse attack against other users of the same system, by creating a program in the system root with the same name as some commonly used program, then waiting for another user to subsequently log onto the system and invoke the program. The Trojan horse program would execute with the user's own privileges, thereby enabling it to take any action that the user could take.



The systems primarily at risk from this vulnerability would be workstations that are shared between multiple users, and local terminal server sessions. Other systems would be at significantly less risk.



**Flaw in Windows XP
Help and Support
Center**

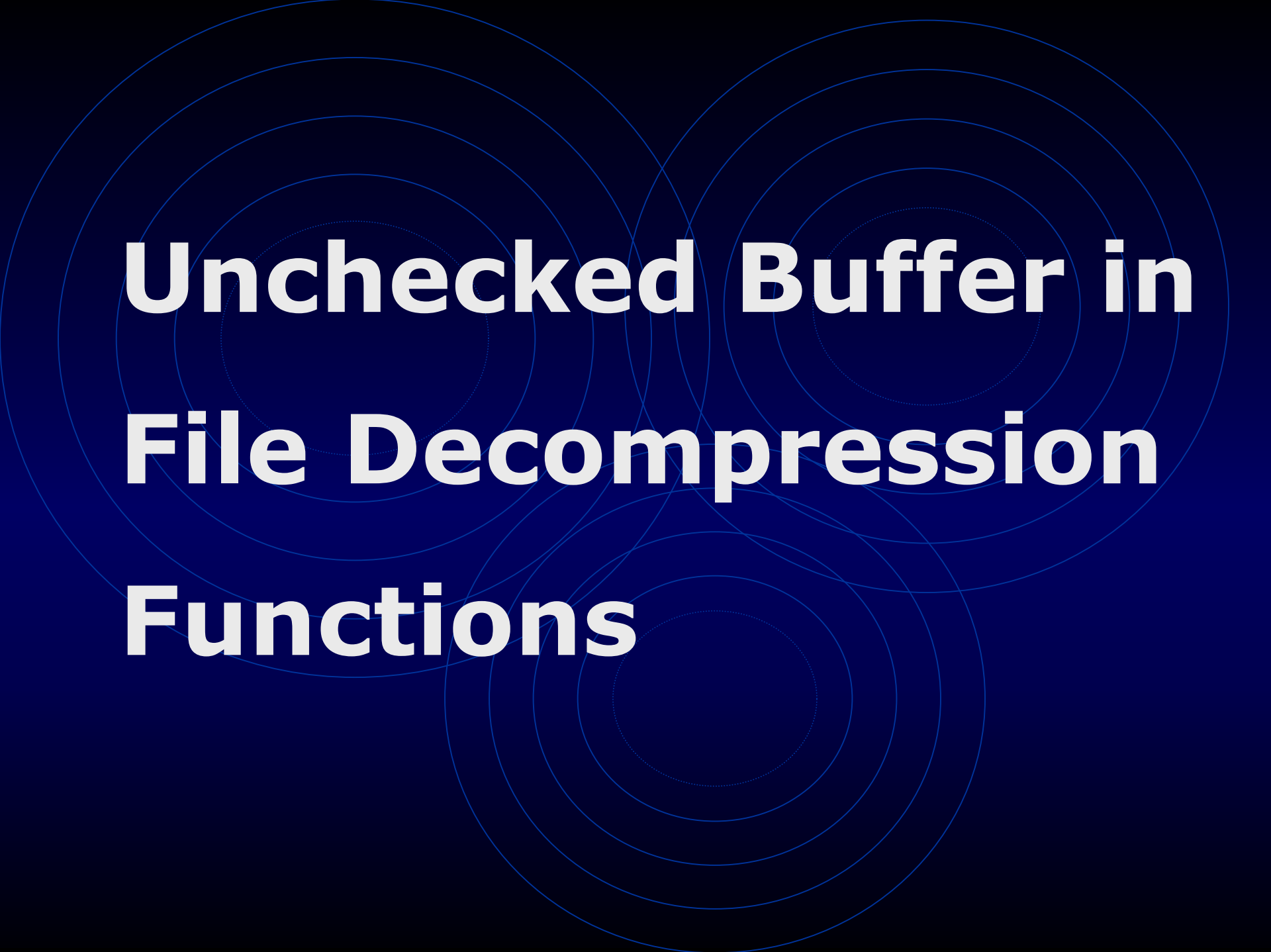
A security vulnerability is present in the Windows XP version of Help and Support Center which could allow an attacker to delete files on the local system by constructing a web page or sending a HTML e-mail.

Issue

Help and Support Center provides a centralized facility through which users can obtain assistance on a variety of topics. For instance, it provides product documentation, assistance in determining hardware compatibility, access to Windows Update, online help from Microsoft, and other assistance.

A security vulnerability is present in the Windows XP version of Help and Support Center, and results because a file intended only for use by the system is instead available for use by any web page. The purpose of the file is to enable anonymous upload of hardware information, with the user's permission, so that Microsoft can evaluate which devices users are not currently finding device drivers for. This information is then used to work with hardware vendors and device teams to improve the quality and quantity of drivers available in Windows. By design, after attempting to upload an XML file containing the hardware information, the system deletes it.

An attacker could exploit the vulnerability by constructing a web page that, when opened, would call the errant function and supply the name of an existing file or folder as the argument. The attempt to upload the file or folder would fail, but the file nevertheless would be deleted. The page could be hosted on a web site in order to attack users visiting the site, or could be sent as an HTML mail in order to attack the recipient when it was opened.



Unchecked Buffer in File Decompression Functions

The ZIP file decompression functions of Windows 98, Me and XP are vulnerable to a buffer overrun attack which could allow an attacker to run the code of their choice on the system.

Issue

Zipped files (files having a .zip extension) provide a means to store information in a way that uses less space on a hard disk. This is accomplished by compressing the files that are put into in the zipped file. On Windows 98 with Plus! Pack, Windows Me and Windows XP, the Compressed Folders feature allows zipped files to be treated as folders. The Compressed Folders feature can be used to create, add files to, and extract files from zipped files.

Two vulnerabilities exist in the Compressed Folders function:

An unchecked buffer exists in the programs that handles the decompressing of files from a zipped file. A security vulnerability results because attempts to open a file with a specially malformed filename contained in a zipped file could possibly result in Windows Explorer failing, or in code of the attacker's choice being run.

The decompression function could place a file in a directory that was not the same as, or a child of, the target directory specified by the user as where the decompressed zip files should be placed. This could allow an attacker to put a file in a known location, such as placing a program in a startup directory.

Affected operating system

- Microsoft Windows 98 with Plus! Pack
- Microsoft Windows Me
- Microsoft Windows XP



Authentication Flaw in Windows Debugger

A security vulnerability in the authentication mechanism for the Windows debugging facility may allow a malicious user to execute the code of their choice in the same security context as a controlled program.

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.

Affected operating system

- **Microsoft Windows NT 4.0**
- **Windows NT 4.0 Terminal Server Edition**
- **Windows 2000**