

Securiteam: [NT] Unchecked Buffer in Windows Shell Could Enable System Compromise (XP)

# [NT] Unchecked Buffer in Windows Shell Could Enable System Compromise (XP)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0065.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 07/17/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 17 Jul 2003 12:05:41 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.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](mailto:canadasales@beyondsecurity.com)

-----  
Unchecked Buffer in Windows Shell Could Enable System Compromise (XP)  
-----

## SUMMARY

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. It 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 programs.

An unchecked buffer exists in one of the functions used by the Windows shell to extract custom attribute information from certain folders. A security vulnerability results because it is possible for a malicious user to construct an attack that could exploit this flaw and execute code on the user's system.

An attacker could seek to exploit this vulnerability by creating a Desktop.ini file that contains a corrupt custom attribute, and then host it on a network share. If a user were to browse the shared folder where the file was stored, the vulnerability could then be exploited. A

## Securiteam: [NT] Unchecked Buffer in Windows Shell Could Enable System Compromise (XP)

successful attack could have the effect of either causing the Windows shell to fail, or causing an attacker's code to run on the user's computer in the security context of the user.

### DETAILS

#### Affected Software:

- \* Microsoft Windows XP

#### Not affected Software:

- \* Microsoft Windows Millennium Edition
- \* Microsoft Windows NT® Server 4.0
- \* Microsoft Windows NT® 4.0, Terminal Server Edition
- \* Microsoft Windows 2000
- \* Microsoft Windows Server 2003

#### Mitigating factors:

\* In the case where an attacker's code was executed, the code would run in the security context of the user. As a result, any limitations on the user's ability would also restrict the actions that an attacker's code could take.

\* An attacker could only seek to exploit this vulnerability by hosting a malicious file on a share.

\* This vulnerability only affects Windows XP Service Pack 1. Users running Windows XP Gold are not affected.

#### Patch availability:

Download locations for this patch

- \* Microsoft Windows XP 32 bit Edition –

<http://microsoft.com/downloads/details.aspx?FamilyId=27D02AF5-A2E1-4E25-9D16-502886161A35&displaylang=en>  
<http://microsoft.com/downloads/details.aspx?FamilyId=27D02AF5-A2E1-4E25-9D16-502886161A35&displaylang=de>

- \* Microsoft Windows XP 64 bit Edition –

<http://microsoft.com/downloads/details.aspx?FamilyId=4BA84E2B-49F9-4416-8745-51F03503AB7D&displaylang=en>  
<http://microsoft.com/downloads/details.aspx?FamilyId=4BA84E2B-49F9-4416-8745-51F03503AB7D&displaylang=de>

#### What's the scope of the vulnerability?

This is a buffer overrun vulnerability. An attacker who successfully exploited the vulnerability could run code of their choice on a user's system. This would enable an attacker to perform any action that the user can perform, within the boundaries set forth by their permission level.

#### What causes the vulnerability?

The vulnerability results because of an unchecked buffer in the component of the Windows shell that automatically reads and applies folder attributes from the Desktop.ini file residing in that folder (if one exists).

#### What could this vulnerability enable an attacker to do?

Successfully exploiting this vulnerability could, in the worst case,

## Securiteam: [NT] Unchecked Buffer in Windows Shell Could Enable System Compromise (XP)

enable an attacker to run code of his or her choice on the user's system. Because the Windows shell runs in the context of the user, the attacker's code would also run as the user. Any limitations on the user's ability to delete, add, or modify data or configuration information would also limit the attacker.

What is a "Desktop.ini" file?

Desktop.ini files store information about how file folders and their contents are to be displayed when a user browses them. Desktop.ini files are not necessary for a folder to be viewed, and do not exist in every folder. If present in the folder, a Desktop.ini file may contain different information depending on the programs that have accessed that folder. For instance; Microsoft Windows Explorer may use a Desktop.ini file to store the name and location of the icon that represents the folder, the text of tool tips to be displayed when the mouse pointer briefly rests over the folder, or how files contained by the folder are to be displayed.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by creating a Desktop.ini file that contains a corrupt attribute and hosting it on a network or Internet share. The attacker could then attempt to lure users to that share.

What is the Windows shell?

The Windows shell provides the basic framework for the Windows user interface and is most commonly experienced as the Windows desktop. The shell provides many functions beyond just the desktop and works to present a consistent look and feel throughout the computing experience. The shell can be used to locate files and folders through Windows Explorer, it can be used to provide a consistent way to start programs through shortcuts on the Start menu, and it can be used to provide a consistent interface through desktop themes and colors.

How does the Windows shell process these file attributes?

The Windows shell is responsible for various actions associated with displaying information about files, folders, and icons. For example, the ability to change the folder view to show thumbnail pictures of files on a computer is provided by the Windows shell. When a folder is opened on a computer that is set to display folder contents as thumbnails, the Windows shell is engaged. It automatically detects this setting, and then it displays the contents of the folder as thumbnails.

What is a thumbnail?

In general, a thumbnail is a greatly reduced version of an image that contains just enough detail for the image to be recognizable. Thumbnails are often used in a gallery view to allow the user to browse and select from a collection of images.

What is wrong with the Windows shell?

The function that allows the Windows shell to automatically extract the display attributes of files and folders contains an unchecked buffer. A

## Securiteam: [NT] Unchecked Buffer in Windows Shell Could Enable System Compromise (XP)

buffer overrun can result if the Windows shell attempts to read a corrupt attribute from a Desktop.ini file.

How is the Windows shell invoked to read file or folder attributes?

The specific function that contains the unchecked buffer is invoked only when the Windows shell attempts to parse the Desktop.ini file for the custom attributes it needs to apply to a folder and its contents. This function is invoked when a folder is opened.

Is it possible for an attacker to exploit this vulnerability directly by using e-mail?

No. A user must browse to a share containing the specially crafted desktop.ini file for this vulnerability to be exploited.

I'm not using Windows XP. Could I be affected by the vulnerability?

No. The flaw is only present in Windows XP Service Pack 1. It does not affect Windows XP Gold or any other version of Windows.

Is there a safe way to delete a file that I suspect might have been created to exploit the vulnerability?

If you suspect that you may have downloaded a Desktop.ini file to your computer that has a corrupt custom attribute, do not attempt to delete the file through Windows Explorer. Opening a folder that contains the file will cause the Windows shell to process it and the vulnerable code to be run. Use the command prompt to remove the corrupt file. To access the command prompt, following these steps:

- \* Click Start, and then click Run.
- \* In the Open box, type cmd.exe, and then click OK. Command prompt will start.
- \* Use the DEL command to specify the path to the file and delete it. For specific information on which switches to use, type DEL /? for help.

What does the patch do?

The patch addresses the vulnerability by imposing proper input validation on the affected Windows shell function.

### ADDITIONAL INFORMATION

The information has been provided by

<mailto:0\_50145\_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C\_US@Newsletters.Microsoft.com>  
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

Securiteam: [NT] Unchecked Buffer in Windows Shell Could Enable System Compromise (XP)

=====  
=====

**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.