

[NT] Windows ANI File Parsing Buffer Overflow (MS05-002)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0054.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 01/12/05

To: list@securiteam.com

Date: 12 Jan 2005 12:01:33 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Windows ANI File Parsing Buffer Overflow (MS05-002)

SUMMARY

eEye Digital Security has discovered a vulnerability in USER32.DLL's handling of Windows animated cursor (.ani) files that will allow a remote attacker to reliably overwrite the stack with arbitrary data and execute arbitrary code.

DETAILS

Because Windows animated cursors can be supplied for use by Internet Explorer, this vulnerability affects any applications that use the Internet Explorer component internally, such as Internet Explorer itself, Word, Excel, PowerPoint, Outlook, Outlook Express, and so on, as well as the Windows shell.

In the case of Internet Explorer, the user's system will be compromised when the user views a website that shows a malformed ANI file referenced via a style sheet in the HTML file. Likewise, a system may be compromised through Outlook and Outlook Express when the user tries to read an HTML e-mail containing a MIME-encoded malformed ANI file and a style sheet referencing the encoded ANI file, invoked using HTML such as < BODY

Securiteam: [NT] Windows ANI File Parsing Buffer Overflow (MS05-002)

style="CURSOR: url('cid:xxxx')" >. In the case of the Windows shell (explorer.exe), exploitation occurs when the user opens a folder containing a malformed ANI file.

This vulnerability also exists in all obsolete versions of the Windows operating system (Windows 95/98/NT4).

Technical Details:

The buffer overflow bug exists in a part of USER32.DLL involved in handling ANI animated cursor files. A partial ANI file format is given below:

```
"RIFF" {(DWORD)Length_of_file}
"ACON"
"LIST" {(DWORD)Length_of_list}
"INFO"
"INAM" {(DWORD)Length_of_title} {szTitle}
"IART" {(DWORD)Length_of_author} {szAuthor}
"anih" {(DWORD)Length_of_AnimationHeader} {AnimationHeaderBlock}
```

Generally, the length of AnimationHeaderBlock should be 36 bytes (0x00000024). The vulnerability is in the handling of the Length_of_AnimationHeader field. This value will be passed as the length argument of memcpy(), in order to copy the contents of AnimationHeaderBlock, but the value is not checked appropriately. The buffer intended to hold the AnimationHeaderBlock is located on the stack, so we can overwrite the return address and exception handler on the stack and jump into the buffer containing our code.

This vulnerability is a separate vulnerability from the ones discovered by <<http://www.securiteam.com/windowsntfocus/6Y00L20C1C.html>> X-focus.

Vendor Status:

Microsoft has released a patch for this vulnerability. The patch is available at:

<<http://www.microsoft.com/technet/security/bulletin/MS05-002.msp>>
<http://www.microsoft.com/technet/security/bulletin/MS05-002.msp>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:dsoeder@eeye.com>> Derek Soeder.

The original article can be found at:

<<http://www.eeye.com/html/research/advisories/AD20050111.html>>
<http://www.eeye.com/html/research/advisories/AD20050111.html>

=====

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

Securiteam: [NT] Windows ANI File Parsing Buffer Overflow (MS05-002)

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.