

[NT] Microsoft Windows Kernel ANI File Parsing Crash and DOS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0107.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/27/04

To: list@securiteam.com

Date: 27 Dec 2004 17:05:07 +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>

Microsoft Windows Kernel ANI File Parsing Crash and DOS Vulnerability

SUMMARY

Parsing a specially crafted ANI file causes the Windows kernel to crash or stop to work properly. An attacker can crash or freeze a target system if he sends a specially crafted ANI file within an HTML page or within an Email.

DETAILS

ANI stands for Windows Animated Cursor and manages many images frames. Two vulnerabilities exist in the Windows kernel when it parses ANI files.

A first vulnerability exists because there is no proper check of the frame number set in the ANI file header. If the Windows kernel try to parse the ANI file (offset 0x78 in the ANI file header) and the frame number is set to 0, the kernel will calculate a wrong address to access and then crash.

A second vulnerability exists because there is (again) no proper check of the rate number set in the ANI file header. Setting this number to 0 causes the windows kernel to use up to all of the system resources and then freeze.

Securiteam: [NT] Microsoft Windows Kernel ANI File Parsing Crash and DOS Vulnerability

More details and POC at

<<http://www.xfocus.net/flashsky/icoExp/index.html>>

<http://www.xfocus.net/flashsky/icoExp/index.html>

ADDITIONAL INFORMATION

The information has been provided by <mailto:fangxing@venustech.com.cn>
Flashsky.

=====

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.