

## Cisco Security Agent and Windows Animated Cursor Stack Overflow Vulnerability (ANI 0-day) exploit

PB403656

### Summary

A vulnerability in Animated Cursor (.ANI) files has been discovered in Microsoft Windows Vista, NT, 2000, 2003, and XP operating systems. This vulnerability can be exploited by a malicious Webpage or HTML e-mail message and results in remote code execution with the privileges of the logged-in user.<sup>1</sup>

This exploit is interesting in that it is essentially identical to exploits targeting a vulnerability patched more than two years ago in MS05-002 (January 2005). Microsoft released a fix at that time, but their patch was incomplete. In that patch, Microsoft checked for the length of the first cursor in a file, and refused to process it if the length was wrong. This current exploit simply adds a second (malformed) cursor after the first (well-formed) cursor in the same file. Since current operating systems such as Microsoft Vista inherited this susceptible code, Vista is also vulnerable to this 2-year-old vulnerability.

This vulnerability has already been exploited in several attacks. Cisco<sup>®</sup> has obtained exploit files, and has confirmed that the Cisco Security Agent is effective in stopping these exploits, using the default security policy configuration. Current supported versions of Cisco Security Agent 4.5.x, 5.0.x, 5.1.x and 5.2.x are all effective in stopping the exploits seen to date.

### Details of the Vulnerability

Details of the vulnerability are documented by Microsoft<sup>1</sup> and by the Computer Incident Response Team (CERT)<sup>2</sup>:

Animated cursors are a feature that allows a series of frames, one after another, to appear at the mouse pointer location instead of a single image, thus producing a short loop of animation. The Animated Cursors feature is designated by the .ani suffix, although Windows Explorer will process ANI files with several different file extensions, such as .ani, .cur, or .ico. A stack buffer overflow vulnerability exists in the way that Microsoft Windows processes malformed animated cursor files; as Windows fails to properly validate the size specified in the ANI header.

An attacker could try to exploit the vulnerability by creating a specially crafted Webpage. An attacker could also create a specially crafted e-mail message and send it to an affected system. Upon viewing a Webpage, previewing or reading a specially crafted message, or opening a specially crafted e-mail attachment, the attacker could cause the affected system to execute code. While animated cursors typically are associated with the .ani file extension, a successful attack is not constrained by this file type.

<sup>1</sup> Microsoft: <http://www.microsoft.com/technet/security/advisory/935423.msp>

<sup>2</sup> CERT Advisory: <http://www.kb.cert.org/vuls/id/191609>

## How Cisco Security Agent Stops the Exploit

Cisco Security Agent default policies contain multiple rules that stop the exploit from doing any damage. No changes to the Cisco Security Agent binaries or default configuration are required to get this protection.

The following actions have been observed being blocked by Cisco Security Agent running the default security policies:

- Execution of a system function from a buffer, through a buffer overflow
- Modification of system files by a recently downloaded application
- Modification of system files
- Execution a command shell by a network process
- Capture of keystrokes by a windows process
- Code injections

This testing is shown in Figure 1.

**Figure 1.** Cisco Security Agent Default Configuration Stops the ANI. 0-Day Exploit (Tested on Cisco Security Agent 5.2)

123	4/2/2007 10:56:54 AM	<a href="#">metasploitxp</a>	Notice	TESTMODE: The process 'C:\WINDOWS\winxp.exe' (as user NT AUTHORITY\SYSTEM) attempted to access a <a href="#">resource</a> which would have resulted in the user being asked the following question. 'The process C:\WINDOWS\winxp.exe is attempting to inject code into the process <call>. Do you wish to allow this?' <a href="#">Details</a>   <a href="#">Rule 189</a>   <a href="#">Wizard</a>	<a href="#">Find Similar</a>
122	4/2/2007 10:56:54 AM	<a href="#">metasploitxp</a>	Notice	TESTMODE: The process 'C:\WINDOWS\winxp.exe' (as user NT AUTHORITY\SYSTEM) attempted to access a <a href="#">resource</a> which would have resulted in the user being asked the following question. 'The process C:\WINDOWS\winxp.exe is attempting to capture keystrokes. Do you wish to allow this?' <a href="#">Details</a>   <a href="#">Rule 184</a>   <a href="#">Wizard</a>	<a href="#">Find Similar</a>
121	4/2/2007 10:56:51 AM	<a href="#">metasploitxp</a>	Notice	TESTMODE: The process 'C:\WINDOWS\system32\cmd.exe' (as user METASPLOITXP\Administrator) attempted to access a <a href="#">resource</a> which would have resulted in the user being asked the following question. 'The process C:\WINDOWS\system32\cmd.exe is attempting to modify the system file C:\WINDOWS\RAV2007.BAT. Do you wish to allow this?' <a href="#">Details</a>   <a href="#">Rule 61</a>   <a href="#">Wizard</a>	<a href="#">Find Similar</a>
120	4/2/2007 10:56:50 AM	<a href="#">metasploitxp</a>	Alert	TESTMODE: The current application 'C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down1.exe' (as user METASPLOITXP\Administrator) attempted to execute the new application 'C:\WINDOWS\system32\cmd.exe'. The operation would have been denied. <a href="#">Details</a>   <a href="#">Rule 461</a>   <a href="#">Wizard</a>	<a href="#">Find Similar</a>
119	4/2/2007 10:56:49 AM	<a href="#">metasploitxp</a>	Notice	TESTMODE: The process 'C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down1.exe' (as user METASPLOITXP\Administrator) attempted to access a <a href="#">resource</a> which would have resulted in the user being asked the following question. 'The process C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down1.exe is attempting to modify the system file C:\WINDOWS\RAV2007.BAT. Do you wish to allow this?' <a href="#">Details</a>   <a href="#">Rule 61</a>   <a href="#">Wizard</a>	<a href="#">Find Similar</a>
118	4/2/2007 10:56:49 AM	<a href="#">metasploitxp</a>	Notice	TESTMODE: The process 'C:\WINDOWS\winxp.exe' (as user NT AUTHORITY\SYSTEM) attempted to access a <a href="#">resource</a> which would have resulted in the user being asked the following question. 'The process C:\WINDOWS\winxp.exe is attempting to modify the system file C:\WINDOWS\winxp.DLL. Do you wish to allow this?' <a href="#">Details</a>   <a href="#">Rule 61</a>   <a href="#">Wizard</a>	<a href="#">Find Similar</a>
117	4/2/2007 10:56:48 AM	<a href="#">metasploitxp</a>	Notice	TESTMODE: The process 'C:\WINDOWS\winxp.exe' (as user NT AUTHORITY\SYSTEM) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINDOWS\winxp.exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' <a href="#">Details</a>   <a href="#">Rule 186</a>   <a href="#">Wizard</a>	<a href="#">Find Similar</a>
116	4/2/2007 10:50:46 AM	<a href="#">metasploitxp</a>	Notice	TESTMODE: The process 'C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down1.exe' (as user METASPLOITXP\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down1.exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' <a href="#">Details</a>   <a href="#">Rule 186</a>   <a href="#">Wizard</a>	<a href="#">Find Similar</a>
115	4/2/2007 10:56:46 AM	<a href="#">metasploitxp</a>	Notice	TESTMODE: The process 'C:\WINDOWS\system32\cmd.exe' (as user METASPLOITXP\Administrator) attempted to access a <a href="#">resource</a> which would have resulted in the user being asked the following question. 'A process is attempting to invoke C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down1.exe which has been recently downloaded and may be dangerous. Do you wish to allow this?' <a href="#">Details</a>   <a href="#">Rule 454</a>   <a href="#">Wizard</a>	<a href="#">Find Similar</a>
114	4/2/2007 10:56:44 AM	<a href="#">metasploitxp</a>	Notice	TESTMODE: The process 'C:\Program Files\Internet Explorer\iexplore.exe' (as user METASPLOITXP\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\Program Files\Internet Explorer\iexplore.exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' <a href="#">Details</a>   <a href="#">Rule 186</a>   <a href="#">Wizard</a>	<a href="#">Find Similar</a>

**Note:** The exploit was tested at Cisco, with the agent in Test mode, which will cause the agent to alert (but not block) malicious behavior. This was done to observe all possible ways that the Cisco Security Agent default policies would stop the exploit. When the agent is in Protect mode (the typical operational configuration), the first rule would kill the exploit: no subsequent events would be seen, since the exploit would be terminated before it could perform any malicious actions.

Testing was performed against the Cisco Security Agent default policies. No binary or policy update was needed for Cisco Security Agents to be effective. In short, this was a true test of "day-zero" protection. This is similar to what Cisco has seen with earlier exploits and worms—the

