



- [About Us](#)
- [Contact Us](#)
- [Advertisement](#)
- [Subscription](#)
- [Download \[Current Issue\]](#)

[Home](#)

[News Briefs](#)

[Cover Story](#)

[Special Focus](#)

[Launch Pad](#)

[Happening](#)

[Product Plus](#)

[Product Review](#)

[New Face](#)

[In Focus](#)

[Corporate Vision](#)

[Corporate Buzz](#)

[Channel Leader](#)

[Solution Provider](#)

[Advanced Search](#)

[Events & Seminars](#)

[Eastern News](#)

[Contact Us](#)

[Download](#)

[Web Link](#)

**Login Form**

Username

Password

Remember me

[Lost Password?](#)

No account yet? [Register](#)

[Submit Web Link](#)

### Upcoming Event

[05.06.2007](#)

**[Computex Taipei-2007](#)**

[June-5-9-2007 Taipei](#)

[Inter...](#)

### Archive

- [February, 2007](#)
- [January, 2007](#)

### Related Topic

[Home](#) [arrow](#) [News Briefs](#) [arrow](#) [Microsoft goes out of cycle to patch cursor vulnerability](#)

Microsoft goes out of  
cycle to patch cursor  
vulnerability

[PDF](#)

[Print](#)

[E-mail](#)

Written by NCN News Network

Security experts at the AntiVirus and Content Security firm MicroWorld Technologies say that new exploits are out on the Internet and are being actively exploited using many malicious websites, while Microsoft Corporation broke its monthly patch cycle and released a security fix yesterday for the critical cursor vulnerability referred to as CVE-2007-1765. The flaw in question is a remote code execution vulnerability that exists in the way Windows handles cursors, animated cursors and icons that use .ani files. These are the files that help changing the cursor into a heart, a bee, a fighter plane, or any other animation.

An attacker can exploit the vulnerability by constructing a tricky cursor that can potentially allow Remote Code Execution when a user visits a malicious website or views a specially crafted e-mail message. If the attacker succeeds in exploiting the vulnerability, he or she can take over the computer and perform operation on it, while in some other cases, it turns out to be a Denial of Service attack by causing continuous system reboots.



Write Comment



Write Comment

- Please keep the topic of messages relevant to the subject of the article.
- Personal verbal attacks will be deleted.
- Please don't use comments to plug your web site. Such material will be removed.
- Just ensure to \*Refresh\* your browser for a new security code to be displayed prior to clicking on the 'Send' button.
- Keep in mind that the above process only applies if you simply entered the wrong security code.

Name:

E-mail:

Web Site:

Comment:

Code:\*

**Code**

I wish to be contacted by email regarding additional comments

[< Prev](#)

[Next >](#)

[\[ Back \]](#)

#### **NCN Newsletter**

Letter:

Name:

Email:

#### **Eastern News**

- [‘GUTS’ get up to sell](#)
- [Logitech Alto Takes Notebook PC Comfort to New Heights](#)
- [Sanyo launches its range of digital cameras in India](#)
- [HP Unveils World’s First Six-Color Photo Scanners](#)
- [Genius Showcased its Design & Technology Capability at CeBIT](#)

[Read More ...](#)

#### **Latest News**

- [Patel Trades provide chip-based recycling technology solutions.](#)
- [Acer ranks No. 1 in Micro-Portable Projectors](#)
- [XEROX strengthens its LASER range in India](#)
- [NETGEAR to Impart Technical Training to Its Channel Partners](#)
- [Samsung Printers Certified as Eco-friendly](#)

## New Face



Rajesh Sahore as Head – Operations (West Zone) -D-Link India Ltd.

[Read more...](#)

## Popular

- [Channel management critical for success](#)
- [10 reasons why deals don't fail!](#)
- [Micronet betting big on India](#)
- [Rashi to promote XFX's 2 new graphic cards in India](#)
- [Changing face of networking](#)



© 2007 Roy Mediative. All rights reserved.

powered by [Excel Software Solutions.](#)

Use Mozilla Firefox 1.0 & above, Best viewed in 1024 \* 768