

[Full-disclosure] 0-day ANI vulnerability in Microsoft Windows (CVE-2007-0038)

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-03/msg00536.html>

- *From:* Alexander Sotirov <asotirov@xxxxxxxxxxxxxx>
 - *Date:* Thu, 29 Mar 2007 22:53:15 -0700
-

Today Microsoft released a security advisory about a vulnerability in the Animated Cursor processing code in Windows:

<http://www.microsoft.com/technet/security/advisory/935423.mspx>

It seems like the vulnerability is already exploited in the wild:

<http://asert.arbornetworks.com/2007/03/any-ani-file-could-infect-you/>

This is one of the vulnerabilities Determina discovered and reported to Microsoft back in December of last year. It was assigned CVE-2007-0038 and we published a brief advisory about it today:

http://www.determina.com/security_center/security_advisories/securityadvisory_0day_032907.asp

The vulnerability is trivially exploitable on all versions of Windows, including Vista. The protected mode of IE7 will lessen the impact of the vulnerability, but shellcode execution is of course still possible. Determina also discovered that under certain circumstances Mozilla Firefox uses the same underlying Windows code for processing ANI files, and can be exploited similarly to Internet Explorer.

As noted in Microsoft's security advisory, workarounds for this vulnerability are limited at this point. I personally recommend browsing the web and reading mail with telnet until patches are available.

Of course, Determina VPS Desktop and Server Edition have been continuously protecting against this vulnerability even prior to its discovery.

Alexander Sotirov
Determina Security Research

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>