

[NT] Microsoft Internet Explorer SVG animateMotion.by Code Execution Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00035.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 13 Feb 2008 09:58:36 +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 Internet Explorer SVG animateMotion.by Code Execution
Vulnerability

SUMMARY

A vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Microsoft Internet Explorer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page.

DETAILS

The specific flaw exists in the handling of the "by" property of an animateMotion SVG element. By assigning other DOM elements to this property, a memory corruption occurs during the destruction of a Variant data type. The corruption causes an overwrite of a virtual function address allowing for the execution of arbitrary code.

Vendor Response:

Microsoft has issued an update to correct this vulnerability. More details can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS08-010.msp>>
<http://www.microsoft.com/technet/security/Bulletin/MS08-010.msp>

[NT] Microsoft Internet Explorer SVG animateMotion.by Code Execution Vulnerability

Disclosure Timeline:

2007.09.17 – Vulnerability reported to vendor

2008.02.12 – Coordinated public release of advisory

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0077>>

CVE-2008-0077

ADDITIONAL INFORMATION

The information has been provided by <<mailto:zdi-disclosures@xxxxxxxx>>

The Zero Day Initiative (ZDI).

The original article can be found at:

<<http://www.zerodayinitiative.com/advisories/ZDI-08-006.html>>

<http://www.zerodayinitiative.com/advisories/ZDI-08-006.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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.