

[NT] Internet Explorer Script Action Handlers (mshtml.dll) Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00053.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 20 Mar 2006 12:43:47 +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>

Internet Explorer Script Action Handlers (mshtml.dll) Buffer Overflow

SUMMARY

mshtml.dll is a module containing HTML-related utility functions.

By crafting specially crafted html, attackers can cause a buffer overflow with mshtml.dll and execute arbitrary code.

DETAILS

Vulnerable Systems:

- * MS Internet Explorer mshtml 6.0.2

This vulnerability can be triggered by specifying more than a couple thousand script action handlers (such as onLoad, onMouseMove, etc) for any single HTML tag. Due to a programming error, Internet Explorer will then attempt to write memory array out of bounds, at an offset corresponding to the ID of the script action handler multiplied by 4 (due to 32-bit address clipping, the result is a small positive integer).

The list of IDs can be found on the Web, and is as follows (values in

[NT] Internet Explorer Script Action Handlers (mshtml.dll) Buffer Overflow

parentheses = resulting offsets):

onhelp = 0x8001177d (+0x45df4)
onclick = 0x80011778 (+0x45de0)
ondblclick = 0x80011779 (+0x45de4)
onkeyup = 0x80011776 (+0x45dd8)
onkeydown = 0x80011775 (+0x45dd4)
onkeypress = 0x80011777 (+0x45ddc)
onmouseup = 0x80011773 (+0x45dcc)
onmousedown = 0x80011772 (+0x45dc8)
onmousemove = 0x80011774 (+0x45dd0)
onmouseout = 0x80011771 (+0x45dc4)
onmouseover = 0x80011770 (+0x45dc0)
onreadystatechange = 0x80011789 (+0x45e24)
onafterupdate = 0x80011786 (+0x45e18)
onrowexit = 0x80011782 (+0x45e08)
onrowenter = 0x80011783 (+0x45e0c)
ondragstart = 0x80011793 (+0x45e4c)
onselectstart = 0x80011795 (+0x45e54)

What happens next depends on the structure of the page in which the malicious tag is embedded, as well as previously visited page and previously initialized extensions (all these factors can be controlled by the attacker).

When the offending page contains no additional elements, and the user is not redirected from elsewhere, the browser will typically crash immediately, because there is no allocated memory at the resulting offset. In all other cases, crashes will typically occur later, due to attempted use of unrelated but corrupted in-memory buffers –for example, when the user attempts to leave or reload the page. Another good example is coming from a page that contains Macromedia Flash – this usually causes the Flash plugin itself to choke on corrupted memory on cleanup.

Proof of Concept:

Note: It may crash your Browser <<http://lcamtuf.coredump.cx/iedie.html>>
<http://lcamtuf.coredump.cx/iedie.html>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:lcamtuf@xxxxxxxxxxxxx>> Michal Zalewski.

=====

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@xxxxxxxxxxxxx

[NT] Internet Explorer Script Action Handlers (mshtml.dll) Buffer Overflow

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.